TUCS

Johan Kopra

Cellular Automata with Complicated Dynamics

TURKU CENTRE *for* COMPUTER SCIENCE

TUCS Dissertations
No 249, December 2019

Cellular Automata with Complicated Dynamics

Johan Kopra

To be presented, with the permission of the Faculty of Science and Engineering of the University of Turku, for public criticism in Auditorium Pub 3 on December 13, 2019, at 12 noon.

University of Turku
Department of Mathematics and Statistics
FI-20014 Turku

2019

Supervisor

Professor Jarkko Kari
Department of Mathematics and Statistics
University of Turku
Finland

Reviewers

Professor Mike Boyle
Department of Mathematics
University of Maryland
USA

Professor Mathieu Sablik
Institut de Mathématiques de Toulouse
Université Paul Sabatier
France

Opponent

Professor Nicolas Ollinger
Laboratoire d'Informatique Fondamentale d'Orléans
Université d'Orléans
France

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the *Turnitin OriginalityCheck* service.

ISBN 978-952-12-3891-8
ISSN 1239-1883

Abstract

A subshift is a collection of bi-infinite sequences (configurations) of symbols where some finite patterns of symbols are forbidden to occur. A cellular automaton is a transformation that changes each configuration of a subshift into another one by using a finite look-up table that tells how any symbol occurring at any possible context is to be changed. A cellular automaton can be applied repeatedly on the configurations of the subshift, thus making it a dynamical system.

This thesis focuses on cellular automata with complex dynamical behavior, with some different definitions of the word "complex". First we consider a naturally occurring class of cellular automata that we call multiplication automata and we present a case study with the point of view of symbolic, topological and measurable dynamics. We also present an application of these automata to a generalized version of Mahler's problem.

For different notions of complex behavior one may also ask whether a given subshift or class of subshifts has a cellular automaton that presents this behavior. We show that in the class of full shifts the Lyapunov exponents of a given reversible cellular automaton are uncomputable. This means that in the dynamics of reversible cellular automata the long term maximal propagation speed of a perturbation made in an initial configuration cannot be determined in general from short term observations.

In the last part we construct, on all mixing sofic shifts, diffusive glider cellular automata that can decompose any finite configuration into two distinct components that shift into opposing direction under repeated action of the automaton. This implies that every mixing sofic shift has a reversible cellular automaton all of whose directions are sensitive in the sense of the definition of Sablik. We contrast this by presenting a family of synchronizing subshifts on which all reversible cellular automata always have a non-sensitive direction.

Tiivistelmä

Siirtoavaruus on kokoelma kahteen suuntaan äärettömiä symbolijonoja (konfiguraatioita), joissa jotkin äärelliset merkkijonot eivät voi esiintyä. Soluautomaatti on transformaatio, joka muuttaa jokaisen siirtoavaruuden konfiguraation toiseksi käyttämällä äärellistä hakutaulukkoa, joka kertoo miten kussakin kontekstissa esiintyvä symboli on muutettava. Soluautomaattia voidaan soveltaa toistuvasti siirtoavaruuden konfiguraatioihin, mikä tekee soluautomaatista dynaamisen systeemin.

Tämä väitöskirja keskittyy soluautomaatteihin joiden dynaaminen käyttäytyminen on kompleksista, joillakin sanan "kompleksinen" määritelmillä. Ensin tarkastelemme luonnollisesti esiintyvää soluautomaattiperhettä, ns. kertolaskuautomaatteja, ja esitämme tapaustutkimuksen symbolidynamiikan sekä topologisen ja mitallisen dynamiikan näkökulmista. Esitämme myös näiden soluautomaattien sovelluksen Mahlerin ongelman yleistettyyn versioon.

Eri kompleksisen käyttäytymisen käsitteitä kohden voidaan myös kysyä, onko jollain annetulla siirtoavaruudella tai siirtoavaruuksien luokalla olemassa soluautomaattia, jolla esiintyy kyseisen tyyppistä käyttäytymistä. Osoitamme, että täysien siirtoavaruuksien luokassa ei ole mahdollista laskea, mitkä ovat annetun kääntyvän soluautomaatin Lyapunov-eksponentit. Tämä tarkoittaa, että kääntyvien soluautomaattien dynamiikassa ei yleisesti ole mahdollista määrittää lyhyen aikavälin havaintojen perusteella, mikä on konfiguraatioon tehdyn perturbaation maksimaalinen pitkän aikavälin kulkunopeus.

Viimeisessä osassa konstruoimme jokaiseen sekoittavaan sofiseen siirtoavaruuteen diffuusiivisen liituriautomaatin, joka voi hajoittaa jokaisen äärellisen konfiguraation kahteen erilliseen komponenttiin, jotka siirtyvät kahteen vastakkaiseen suuntaan, kun soluautomaattia käytetään toistuvasti. Tästä seuraa, että jokaisella sekoittavalla sofisella siirtoavaruudella on kääntyvä soluautomaatti, jonka kaikki suunnat ovat sensitiivisiä Sablikin määritelmän mielessä. Kontrastiksi tälle esitämme perheen synkronoivia siirtoavaruuksia, joiden kaikilla kääntyvillä soluautomaateilla on aina epäsensitiivinen suunta.

Acknowledgements

This thesis is the end result of not only my efforts but also both the intentional and unintentional support of several people. In the following I mention some of the people involved in the process.

First I thank my supervisor Professor Jarkko Kari, who also supervised my master's thesis. When I was probing the possibility of him supervising my doctoral dissertation, I may have done so in a very roundabout way. Nevertheless he understood my intention and introduced me to the topic of multiplication automata and suggested to me questions concerning them. Some of these questions are answered in the third chapter of this thesis, but later chapters represent a divergence from the initial topic.

I am grateful to Professor Mike Boyle and Professor Mathieu Sablik for reviewing my thesis and to Professor Nicolas Ollinger for agreeing to act as my opponent.

I thank the MATTI doctoral program and the Vilho, Yrjö and Kalle Väisälä Foundation of the Finnish Academy of Science and Letters for their financial support.

As I was completing my master's thesis, I had no plans for what to do after graduating. I thank the former head of the department Professor Juhani Karhumäki, who recommended me to apply for the MATTI doctoral program. The thought of pursuing doctoral studies may not have occurred to me otherwise.

I initially started my studies at the University of Turku as a chemistry student. In my first year I took the analysis courses given by Docent Jyrki Lahtonen, during which I became interested in mathematics. In my second year I took the linear algebra course given by Professor Tero Laihonen, during which I decided to switch my major to mathematics. I gratefully acknowledge their early influence.

Doctor Michal Szabados shared an office with me for the first semester of my graduate studies. I appreciate him for trying to explain his ideas on many occasions. I got from him my first glimpse on how research in mathematics is done (I am still trying to get the hang of it myself). I am also grateful to him for initiating me into the departmental coffee breaks. Without these breaks I would have had less fun (and perhaps had been more productive).

I wish to thank Doctor Ville Salo for his expositions on cellular automata, topological dynamical systems and mathematics in general. They have certainly influenced my thinking. I also appreciate his patience on the times I have not been able to instantly understand his explanations. In addition I thank him for helpful discussions without which the results of Chapter 5 would not be quite as general.

Joonatan Jalonen started his graduate studies under the supervision of Jarkko at the same time as me. Special thanks goes to him for presenting me with a puzzle to which I answered by constructing the cellular automaton in Subsection 5.1.1. No trace of Chapter 5 would exist without this prompt.

Finally, I am grateful to my big sister Eila for her encouragement in moments of self doubt and to my whole family for all their love and support.

Turku, November 11, 2019
Johan Kopra

List of original publications

1. Jarkko Kari and Johan Kopra. Cellular automata and powers of p/q. *RAIRO-Theoretical Informatics and Applications*, 51(4):191–204, 2017.

2. Johan Kopra. Glider automorphisms on some shifts of finite type and a finitary Ryan's theorem. In *International Workshop on Cellular Automata and Discrete Complex Systems*, pages 88–99. Springer, 2018.

3. Johan Kopra. The Lyapunov exponents of reversible cellular automata are uncomputable. In *International Conference on Unconventional Computation and Natural Computation*, pages 178–190. Springer, 2019.

4. Johan Kopra. Glider automorphisms and a finitary Ryan's theorem for transitive subshifts of finite type. *Natural Computing*, Sep 2019.

Contents

Chapter 1

Introduction

The results in this thesis are motivated by two related goals. First, we wanted to find complex or interesting reversible cellular automata in various subshifts. On the other hand, we wanted to find some general conditions under which one might expect to find such automata. We present partial results related to these goals. We begin with an overview on the subject of cellular automata.

A basic object in symbolic dynamics is a *configuration*, i.e. a uniform discrete lattice of cells each of which contains a state from some finite set A. In our considerations the lattice is the one-dimensional array of integers $\mathbb{Z}$, in which case the set of configurations is $A^{\mathbb{Z}}$. The value of $x \in A^{\mathbb{Z}}$ at coordinate $i \in \mathbb{Z}$ is denoted by $x[i] \in A$. We interpret the lattice $\mathbb{Z}$ to be a "world" and a configuration $x \in A^{\mathbb{Z}}$ to be some determination of the contents of the world at each coordinate. A *cellular automaton* (CA) is a function $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ which gives laws of physics to the world: if x tells what the world looks like at time step 0, then $F^t(x)$ tells what the world looks like at time step t. The laws of physics given by F are local and independent of the position in the lattice $\mathbb{Z}$. More formally, this means that for every CA F there is a number $r \in \mathbb{N}$ and a function $f : A^{2r+1} \to A$ (a *local rule*) such that

$$F(x)[i] = f(x[i-r], \dots, x[i], \dots, x[i+r]) \text{ for all } x \in A^{\mathbb{Z}}, i \in \mathbb{Z}.$$

The fact that every CA F can be represented by a local rule f turns cellular automata into finitary and combinatorial objects.

A simple example is the *traffic rule* cellular automaton $W_{184} : \{0,1\}^{\mathbb{Z}} \to \{0,1\}^{\mathbb{Z}}$. A typical fragment of a configuration is represented as the first row of Figure 1.1. This row, the "world", is interpreted as a lane of a road viewed from the side and each occurrence of the digit 1 is interpreted as a vehicle. The CA W_{184} encodes the laws of physics (in this case more properly laws of the road) which say that a vehicle will travel to the right at a constant

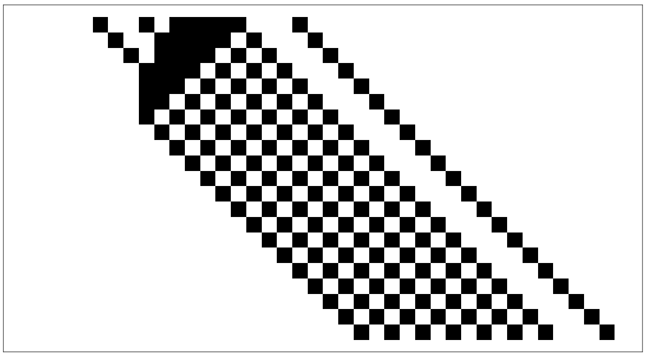

Figure 1.1: A traffic jam as represented by the cellular automaton W_{184}. White and black squares correspond to digits 0 and 1 respectively.

speed unless a traffic jam is encountered, in which case the vehicle will wait until the jam clears up. In Figure 1.1 the state of the road at consecutive time steps is represented on consecutive rows in a *space-time diagram.*

The main focus on this thesis will be on reversible automata. What this means precisely is that the cellular automata functions $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ that we consider are bijections. Focusing on reversible CA is motivated for example by the fact that the laws of physics of the real world also seem to be reversible. The non-reversibility of a CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ often manifests itself in simulations by unaccounted loss of energy. For example the traffic rule W_{184} does not take into account the dissipation of kinetic energy into heat when the vehicles slow down in anticipation of traffic jams, and indeed it can be shown that W_{184} is not bijective (it is not even surjective).

An example of a reversible CA is the *shift map* $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ that shifts all symbols by one position to the left, i.e. $\sigma(x)[i] = x[i+1]$ for $x \in A^{\mathbb{Z}}$, $i \in \mathbb{Z}$. More complicated reversible CA can be constructed as compositions of partial shifts and symbol permutations. If our symbol set is a cartesian product $A = A_1 \times A_2$, then a configuration $x \in A^{\mathbb{Z}}$ can be interpreted as consisting of two tracks $x_1 \in A_1^{\mathbb{Z}}$ and $x_2 \in A_2^{\mathbb{Z}}$ where $x[i] = (x_1[i], x_2[i])$ for $i \in \mathbb{Z}$. Therefore we may identify x with the pair (x_1, x_2) and we can define a *partial shift* $\tau : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $\tau(x) = (\sigma(x_1), x_2)$. A *partitioned cellular automaton* (PCA) is a composition $\pi \circ \tau$, where π is a permutation of A that is applied coordinatewise on configurations of $A^{\mathbb{Z}}$. This is reversible as a composition of two reversible maps. For a recent survey on reversible CA, see [34].

A cellular automaton gives “temporal” laws of physics in the world $\mathbb{Z}$. As noted in [9], it is sometimes natural to also take into account local spatial restrictions, i.e. we allow only some subset $X \subseteq A^{\mathbb{Z}}$ of imaginable contents of the world, a *subshift.* The time-dependencies are also in this case encoded into a CA $F : X \to X$, defined only on X. Depending on the nature of

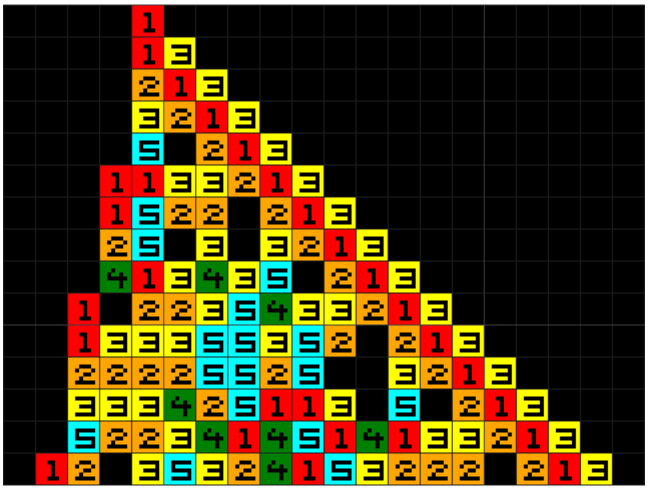

Figure 1.2: A space-time diagram of a finite configuration with respect to the multiplication automaton $\Pi_{3/2,6}$. The 0-digit is denoted by a black square.

spatial restrictions encoded by the subshift X, the group of reversible CA on X can either be complicated (see e.g. [10], this often happens when the action of σ on X is qualitatively similar to its action on $A^{\mathbb{Z}}$) or "small" (see e.g. [15], this often happens when X is in some sense simple).

Multiplication automata are a natural class of interesting reversible CA that have been studied earlier in [5, 48]. If we denote by Σ_n the alphabet containing the digits $\{0, 1, \dots, n-1\}$, then $\Pi_{\alpha,n} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ is the cellular automaton that performs multiplication by α on the base-n representations of nonnegative real numbers. Such automata exist whenever $\alpha = p/q$ and $p, q > 0$ are integers that are products of prime factors of n. For example, the automaton $\Pi_{3/2,6}$ is a *universal pattern generator*: all finite sequences over Σ_6 occur somewhere in its space-time diagram whenever initialized on a configuration with finitely many (and at least one) non-zero digits [23, 32, 33]. An example of a space-time diagram of this CA is in Figure 1.2.

Multiplication automata that are universal pattern generators exist on all configuration spaces $\Sigma_n^{\mathbb{Z}}$ precisely whenever n is not a power of a prime number. It is noteworthy that the proof of this is not combinatorial even though cellular automata are combinatorial objects: the proof in [32] of the result that $\Pi_{3/2,6}$ is a universal pattern generator uses the fact that $\log_6 3$ is irrational. Furthermore, all known universal pattern generators are multiplication automata on some configuration space. It is not known whether there are universal pattern generators on other configuration spaces. We feel that giving a combinatorial explanation of the pattern generation property of multiplication automata could help us determine whether universal pattern generators could be constructed on all full shifts based on some idea that is

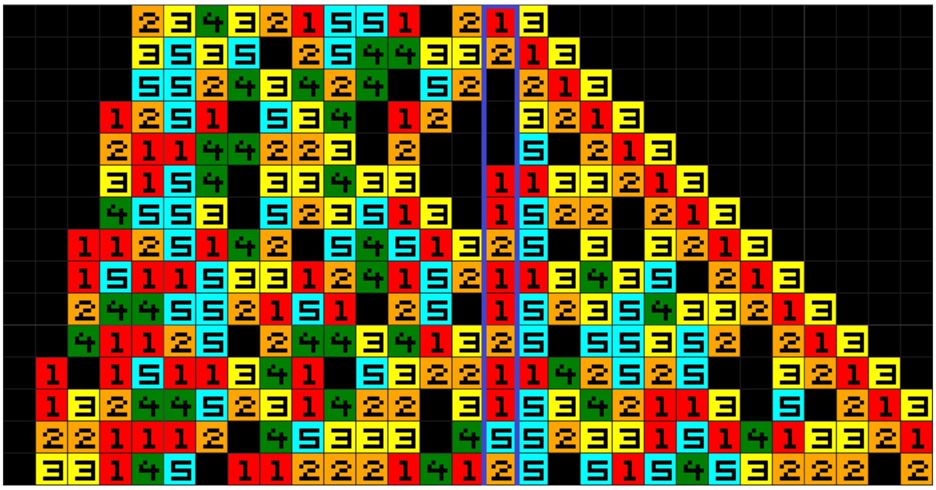

Figure 1.3: A space-time diagram of a configuration x (with respect of $\Pi_{3/2,6}$) that initially seems to be a base-6 representation of a Z-number. Note however an occurrence of the digit 5 on the fourteenth row in the highlighted column.

not number theoretical. We are not able to give such an explanation. In an effort to get closer to this goal, in Chapter 3 we perform an extended case study on multiplication automata. We use mostly combinatorial methods to prove other dynamical properties of interest.

Multiplication by proper fractions $p/q > 0$ (p and q coprime positive integers, $q > 1$) is connected to difficult problems in uniform distribution theory. Denote the fractional part of $\xi \in \mathbb{R}$ by $\mathrm{frac}(\xi)$. It follows from a result of Weyl [60] that the sequence $(\mathrm{frac}(\xi(p/q)^i))_{i\in\mathbb{N}}$ is dense (even uniformly distributed) on the unit interval $[0,1)$ for almost all $\xi \in \mathbb{R}$. On the other hand, concrete examples of such numbers ξ for any fixed p/q are difficult to come by: it is not even known whether $(\mathrm{frac}((3/2)^i))_{i\in\mathbb{N}}$ is dense on $[0,1)$. In the other direction, Mahler [45] asked whether there exist *Z-numbers*, i.e. numbers $\xi > 0$ such that $\mathrm{frac}(\xi(3/2)^i) \in [0,1/2)$ for all i. As noted in [32], questions of this type can be reformulated as problems related to the properties of the CA $\Pi_{p/q,pq}$. For example, note that $\mathrm{frac}(\xi) \in [0,1/2)$ is equivalent to saying that the base-6 representation of ξ contains one of the digits $0,1$ or 2 directly to the right of the decimal point. Therefore the existence of Z-numbers is equivalent to the existence of a configuration $x \in \Sigma_6^{\mathbb{Z}}$ such that $x[i] = 0$ for all sufficiently small i and that the space-time diagram of x with respect to $\Pi_{3/2,6}$ has a column containing only the digits $0,1$ or 2 (see Figure 1.3). Our combinatorial study of the multiplication automata allows us to prove results related to Mahler's problem. Chapter 3 is an extended version of the paper [35].

From the computational point of view one can say that reversible CA on full shifts can exhibit a range of complex behavior because many questions concerning their asymptotic behavior are computationally undecidable. One example is the *local immortality problem*. Given a CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ and a state set $B \subseteq A$ we say that a configuration $x \in A^{\mathbb{Z}}$ is locally immortal (with respect to F and B) if the space-time diagram of x with respect to F has a column containing only symbols from the set B. This relates to Mahler's problem, because the existence of Z-numbers is equivalent to the existence of a configuration $x \in \Sigma_6^{\mathbb{Z}}$, with $x[i] = 0$ for all sufficiently small i, that is locally immortal with respect to the CA $\Pi_{3/2,6}$ and the state set $\{0, 1, 2\}$. It is a result of Lukkarila [44] that the local immortality problem is undecidable for reversible cellular automata. We feel that the difficulty of Mahler's problem is partially explained by the fact that it is "almost" an instance[1] of the local immortality problem, which is undecidable in general.

In Chapter 4 we adapt Lukkarila's argument to prove a directional variant of the undecidability of local immortality. Then we prove as a corollary that the Lyapunov exponents of reversible CA cannot be computed to arbitrary precision. The Lyapunov exponents of a CA F tell the maximal asympotic speed of information propagation in configurations under the action of F, and they are one topological measure of complexity of F. Chapter 4 is based on the paper [39].

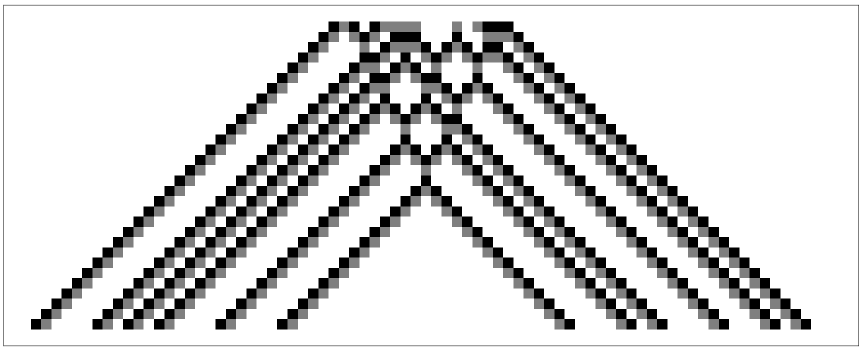

Figure 1.4: The space-time diagram of a finite initial configuration with respect to a diffusive glider CA $G : \Sigma_3^{\mathbb{Z}} \to \Sigma_3^{\mathbb{Z}}$. White, gray and black squares correspond to digits 0, 1 and 2 respectively.

It can be shown that multiplication automata of the form $\Pi_{p,n} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$, where p is a factor of n, are partitioned CA (up to replacing Σ_n by the cartesian product $\Sigma_p \times \Sigma_{n/p}$). One reason why it is not as easy to construct complex reversible CA on other subshifts is that the notion of PCA is not meaningful in general subshifts: consider for example the binary

[1] The reason why this is not precisely true is that Mahler's problem only concerns those configurations that represent positive real numbers.

configuration space $\Sigma_2^{\mathbb{Z}}$, whose symbol set Σ_2 cannot be represented as a nontrivial cartesian product. This indicates that on more general subshifts we should look for sensible analogues of partial shift maps. In Chapter 5 we define a class of reversible CA we call *diffusive glider CA* and we prove that they exist on all mixing sofic shifts (and in particular on all full shifts). Intuitively a diffusive glider CA $G : X \to X$ eventually turns any finite configuration into distinct fleets of gliders that travel at different speeds under the action of G. Space-time diagrams with respect to them look very similar to the space-time diagrams with respect to partial shifts, see Figure 1.4. As an application we prove a finitary Ryan's theorem for mixing sofic shifts: there is a set S containing two reversible CA on X (one of them is a diffusive glider CA) such that the only reversible CA commuting with both elements of S are the shift maps. This chapter is an extended version of the papers [37, 38].

In Chapter 5 we will also have occasion to consider other notions of complexity for cellular automata. Any subshift $X \subseteq A^{\mathbb{Z}}$ has a natural topology under which two points $x, y \in X$ are near each other whenever they agree in a large neighborhood of the origin. Then any CA $F : X \to X$ is a continuous map and the pair (X, F) is a topological dynamical system. It is natural to consider a CA F to be complex in a topological sense if it satisfies some chaotic property such as being sensitive. (In popular accounts a sensitive system is said to exhibit the "butterfly effect".) A downside to this approach is that the shift map $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$, which intuitively seems very simple, satisfies all the typical topological chaoticity properties. To correct this, the framework of directional dynamics was introduced by Sablik in [51], which allows to speak of dynamical properties with respect to a fixed modulus of shift. Then we can say that σ has a non-sensitive direction along which σ looks like the identity map, see Figure 1.5. Our construction of diffusive glider CA shows in particular that all mixing sofic subshifts X have reversible CA that are sensitive with respect to all directions. We complement this result by giving a class of examples of synchronizing subshifts on which all reversible CA have a non-sensitive direction.

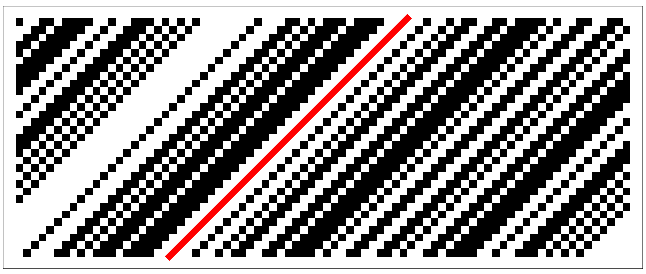

Figure 1.5: A space-time diagram of the binary shift map σ. A direction of non-sensitivity is indicated by a red line.

Chapter 2

Preliminaries

For sets A and B we denote by B^A the collection of all functions from A to B.

2.1 Topological Dynamical Systems

It is natural to consider cellular automata and subshifts in the context of general topological dynamics. We cover here some of the basic notions. For more details, see e.g. the book [42].

Definition 2.1.1. If X is a compact metrizable topological space and $T : X \to X$ is a continuous map, we say that (X, T) is a *(topological) dynamical system*.

When there is no risk of confusion, we may identify the dynamical system (X, T) with the underlying space or the underlying map, so we may say that X is a dynamical system or that T is a dynamical system.

Compact metrizable spaces have several nice properties. For example, every sequence in a compact metrizable space X has a converging subsequence and a subset $A \subseteq X$ is compact if and only if it is closed. If $\mathrm{dist} : X \times X \to X$ is a metric inducing the topology of X, $x \in X$ and $r > 0$, the ball of radius r centered on x is $B_r(x) = \{y \in X \mid \mathrm{dist}(y, x) < r\}$. We do not include the actual metric in this notation. Typically its choice is obvious or irrelevant.

The structure preserving transformations between topological dynamical systems are known as morphisms.

Definition 2.1.2. We write $\psi : (X, T) \to (Y, S)$ whenever (X, T) and (Y, S) are dynamical systems and $\psi : X \to Y$ is a continuous map such that $\psi \circ T = S \circ \psi$ (this equality is known as the *equivariance condition*). Then we say that ψ is a *morphism*. If ψ is injective, we say that ψ is an *embedding*. If ψ is surjective, we say that ψ is a *factor map* and that (Y, S)

is a factor of (X, T) (via the map ψ). If ψ is bijective, we say that ψ is a *conjugacy* and that (X, T) and (Y, S) are *conjugate* (via ψ).

Definition 2.1.3. A morphism $\psi : (X, T) \to (X, T)$ is an *endomorphism* of (X, T) and the set of endomorphisms of (X, T) is denoted by $\mathrm{End}(X, T)$. It is a monoid with respect to function composition. A conjugacy $\psi : (X, T) \to (X, T)$ is an *automorphism* of (X, T) and the set of automorphisms of (X, T) is denoted by $\mathrm{Aut}(X, T)$. It is a group with respect to function composition.

There are several ways to define chaos for dynamical systems. As an example we present a definition of chaos by Devaney.

Definition 2.1.4. (X, T) is *sensitive*, if

$$\exists \epsilon > 0, \forall x \in X, \forall \delta > 0, \exists y \in B_\delta(x), \exists n \in \mathbb{N}, \mathrm{dist}(T^n(y), T^n(x)) > \epsilon.$$

Definition 2.1.5. (X, T) is *transitive*, if for all nonempty open sets $U, V \subseteq X$ there exists $n \in \mathbb{N}$ such that $T^n(U) \cap V \neq \emptyset$.

Definition 2.1.6. Given a dynamical system (X, T), a point $x \in X$ is *periodic* if there exists $p \in \mathbb{N}_+$ such that $T^p(x) = x$.

Definition 2.1.7 (Devaney [14])**.** A dynamical system (X, T) is *chaotic* if it is sensitive, transitive and the set of periodic points is dense in X.

The three criteria of chaoticity mean respectively that the system has elements of unpredictability, indecomposability and regularity.

Stability of a dynamical system is encoded by the notion of equicontinuity.

Definition 2.1.8. Given a dynamical system (X, T), a point x is *equicontinuous* if

$$\forall \epsilon > 0, \exists \delta > 0, \forall y \in B_\delta(x), \forall n \in \mathbb{N}, \mathrm{dist}(T^n(y), T^n(x)) < \epsilon.$$

We say that (X, T) is equicontinuous if all of its points are equicontinuous. We say that (X, T) is *almost equicontinuous* if the set of equicontinuity points is residual (i.e. it contains a countable intersection of open dense sets).

2.2 Combinatorics on Words

A finite set A containing at least two elements (*letters*) is called an *alphabet*. Occasionally we want the alphabet to consist of numbers and thus for $n \in \mathbb{N}_+$ we denote $\Sigma_n = \{0, 1, \ldots, n-1\}$. The set $A^{\mathbb{Z}}$ of bi-infinite sequences (*configurations*) over A is called a *full shift*. Formally any $x \in A^{\mathbb{Z}}$ is a function

$\mathbb{Z} \to A$ and the value of x at $i \in \mathbb{Z}$ is denoted by $x[i]$. It contains finite, right-infinite and left-infinite subsequences denoted by $x[i,j] = x[i]x[i+1]\cdots x[j]$, $x[i,\infty] = x[i]x[i+1]\cdots$ and $x[-\infty,i] = \cdots x[i-1]x[i]$. Occasionally we signify the symbol at position zero in a configuration x by a dot as follows:

$$x = \cdots x[-2]x[-1].x[0]x[1]x[2]\cdots.$$

A configuration $x \in A^{\mathbb{Z}}$ is *periodic* if there is a $p \in \mathbb{N}_+$ such that $x[i+p] = x[i]$ for all $i \in \mathbb{Z}$. Then we may also say that x is p-periodic or that x has period p. If x is not periodic, it is *aperiodic*. We say that x is *eventually periodic* to the right (respectively, to the left) if there is a $p \in \mathbb{N}_+$ such that $x[i+p] = x[i]$ holds for all sufficiently large $i \in \mathbb{Z}$ (respectively, for all sufficiently small $i \in \mathbb{Z}$). If x is eventually periodic to the right, we may just say that x is eventually periodic.

A *subword* of $x \in A^{\mathbb{Z}}$ is any finite sequence $x[i,j]$ where $i,j \in \mathbb{Z}$, and we interpret the sequence to be empty if $j < i$. Any finite sequence $w = w[1]w[2]\cdots w[n]$ (also the empty sequence, which is denoted by ϵ) where $w[i] \in A$ is a *word* over A. Unless we consider a word w as a subword of some configuration, we start indexing the symbols of w from 1 as we have done here. The concatenation of a word or a left-infinite sequence u with a word or a right-infinite sequence v is denoted by uv. A word u is a *prefix* of a word or a right-infinite sequence x if there is a word or a right-infinite sequence v such that $x = uv$. Similarly, u is a *suffix* of a word or a left-infinite sequence x if there is a word or a left-infinite sequence v such that $x = vu$. The set of all words over A is denoted by A^*, and the set of non-empty words is $A^+ = A^* \setminus \{\epsilon\}$. The set of words of length n is denoted by A^n. For a word $w \in A^*$, $|w|$ denotes its length, i.e. $|w| = n \iff w \in A^n$. For any word $w \in A^+$ we denote by ${}^\infty w$ and w^∞ the left- and right-infinite sequences obtained by infinite repetitions of the word w. We denote by $w^{\mathbb{Z}} \in A^{\mathbb{Z}}$ the configuration defined by $w^{\mathbb{Z}}[in,(i+1)n-1] = w$ (where $n = |w|$) for every $i \in \mathbb{Z}$. We say that $x \in A^{\mathbb{Z}}$ is *w-finite* if $x[-\infty,i] = {}^\infty w$ and $x[j,\infty] = w^\infty$ for some $i,j \in \mathbb{Z}$. In the full shift $\Sigma_n^{\mathbb{Z}}$ we say that $x \in \Sigma_n^{\mathbb{Z}}$ is finite if it is 0-finite.

Any collection of words $L \subseteq A^{\mathbb{Z}}$ is called a *language*. For any $S \subseteq A^{\mathbb{Z}}$ the collection of words appearing as subwords of elements of S is the language of S, denoted by $L(S)$. For $n \in \mathbb{N}$ we denote $L^n(S) = L(S) \cap A^n$. The *complexity function* of S is the map $P_S : \mathbb{N} \to \mathbb{N}$ defined by $P_S(n) = |L^n(S)|$ for $n \in \mathbb{N}$. For any $L \subseteq A^*$, let

$$L^* = \{w_1 \cdots w_n \mid n \geq 0, w_i \in L\} \subseteq A^*,$$

i.e. L^* is the set of all finite concatenations of elements of L. If $\epsilon \notin L$, define $L^+ = L^* \setminus \{\epsilon\}$ and if $\epsilon \in L$, define $L^+ = L^*$.

Given $x \in A^{\mathbb{Z}}$ and $w \in A^+$ we define the sets of left (resp. right) occurrences of w in x by

$$\begin{aligned} &\mathrm{occ}_\ell(x,w) = \{i \in \mathbb{Z} \mid x[i, i+|w|-1] = w\} \\ \text{(resp.)} \quad &\mathrm{occ}_r(x,w) = \{i \in \mathbb{Z} \mid x[i-|w|+1, i] = w\}. \end{aligned}$$

Note that both of these sets contain the same information up to a shift in the sense that $\mathrm{occ}_r(x,w) = \mathrm{occ}_\ell(x,w) + |w| - 1$. Typically we refer to the left occurrences and we say that $w \in A^n$ *occurs* in $x \in A^{\mathbb{Z}}$ at position i if $i \in \mathrm{occ}_\ell(x,w)$.

For $x, y \in A^{\mathbb{Z}}$ and $i \in \mathbb{Z}$ we denote by $x \otimes_i y \in A^{\mathbb{Z}}$ the "gluing" of x and y at i, i.e. $(x \otimes_i y)[-\infty, i-1] = x[-\infty, i-1]$ and $(x \otimes_i y)[i, \infty] = y[i, \infty]$. Typically we perform gluings at the origin and we denote $x \otimes y = x \otimes_0 y$.

2.3 Symbolic Dynamics

For a general reference on symbolic dynamics, see [43].

To consider topological dynamics on subsets of the full shift, the set $A^{\mathbb{Z}}$ is endowed with the product topology (with respect to the discrete topology on A). This is a compact metrizable space with one possible metric

$$\mathrm{dist}(x,y) = 2^{-\min\{|i| \mid x[i] \neq y[i], i \in \mathbb{Z}\}}.$$

The shift map $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is defined by $\sigma(x)[i] = x[i+1]$ for $x \in A^{\mathbb{Z}}$, $i \in \mathbb{Z}$, and it is a homeomorphism. Any topologically closed *nonempty* subset $X \subseteq A^{\mathbb{Z}}$ such that $\sigma(X) = X$ is called a *subshift*. It is also a compact metric space under the subspace topology induced from $A^{\mathbb{Z}}$. Any $w \in L(X) \setminus \epsilon$ and $i \in \mathbb{Z}$ determine a *cylinder* of X

$$\mathrm{Cyl}_X(w,i) = \{x \in X \mid w \text{ occurs in } x \text{ at position } i\}.$$

Every cylinder is an open set of X and the collection of all cylinders

$$\mathcal{C}_X = \{\mathrm{Cyl}_X(w,i) \mid w \in L(X) \setminus \epsilon, i \in \mathbb{Z}\}$$

form a basis for the topology of X. The restriction of σ to X is also a homeomorphism and it may be denoted by σ_X. Typically the subscript X is omitted from all notations when X is clear from the context. Every subshift X is identified with the dynamical system (X, σ) induced by the shift map σ.

Subshifts have also the following combinatorial definition. Every collection $\mathcal{F} \subseteq A^{\mathbb{Z}}$ determines a subshift with *forbidden words* $\mathcal{F}$ by

$$X_{\mathcal{F}} = \{x \in A^{\mathbb{Z}} \mid \text{No words of } \mathcal{F} \text{ occur in } x\}.$$

All these sets are indeed subshifts, and furthermore every subshift can be defined by some set of forbidden words. We define some common types of subshifts.

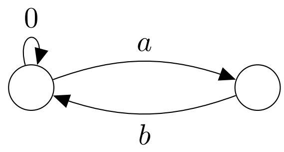

Figure 2.1: The golden mean shift.

Definition 2.3.1. A subshift $X \subseteq A^{\mathbb{Z}}$ is a *shift of finite type* (SFT) if there is a finite set $\mathcal{F} \subseteq A^{\mathbb{Z}}$ such that $X = X_{\mathcal{F}}$. If X can be defined by choosing $\mathcal{F} \subseteq A^{n+1}$ for $n > 0$, we say that X is an n-step SFT and that X is defined by a set of *allowed words* $A^{n+1} \setminus \mathcal{F}$.

An alternative way to define SFTs is by using graphs.

Definition 2.3.2. A (directed) *graph* is a pair $\mathcal{G} = (V, E)$ where V is a finite set of *vertices* (or *nodes* or *states*) and E is a finite set of *edges* or *arrows*. Each edge $e \in E$ starts at an initial state denoted by $\iota(e) \in V$ and ends at a terminal state denoted by $\tau(e) \in V$. We say that $e \in E$ is an outgoing edge of $\iota(e)$ and an incoming edge of $\tau(e)$.

Definition 2.3.3. For any graph $\mathcal{G} = (V, E)$ we call the set

$$\{x \in E^{\mathbb{Z}} \mid \tau(x[i]) = \iota(x[i+1]) \text{ for all } i \in \mathbb{Z}\}$$

(i.e. the set of bi-infinite paths on $\mathcal{G}$) the *edge subshift* of $\mathcal{G}$.

It is known that every SFT is conjugate to some edge subshift.

Example 2.3.4. Let $A = \{0, a, b\}$. The graph in Figure 2.1 defines an SFT X also known as the *golden mean shift*. A typical point of X looks like

$$\cdots 000abab0ab00ab000 \cdots$$

i.e. the letter b cannot occur immediately after 0 or b and every occurrence of a is followed by b.

Definition 2.3.5. A subshift X is a *sofic shift* if it is a factor of an SFT.

By definition it follows that the class of sofic shifts is closed with respect to taking subshift factors. There are many characterizations for the class of sofic shifts. The most popular alternative characterization is that X is sofic if its language $L(X)$ is regular.

Definition 2.3.6. The *orbit* of a point $x \in A^{\mathbb{Z}}$ is $\mathcal{O}(x) = \{\sigma^i(x) \mid i \in \mathbb{Z}\}$. The *orbit closure* of x is $\overline{\mathcal{O}(x)}$, and it is always a subshift.

Unlike on full shifts, on a more general subshift X one cannot glue points $x, y \in X$ in an arbitrary way and expect that the resulting configuration still belongs to X. The following definition introduces two common gluing properties of subshifts.

Definition 2.3.7. We say that a subshift X is *transitive* if for all words $u, v \in L(X)$ there is $w \in L(X)$ such that $uwv \in L(X)$. We say that X is *mixing* if for all $u, v \in L(X)$ there is $N \in \mathbb{N}$ such that for all $n \geq N$ there is $w \in L^n(X)$ such that $uwv \in L(X)$. If it is possible to choose N independently of u and v we say that N is a mixing constant of X.

Given a subshift $X \subseteq A^{\mathbb{Z}}$ and a word $w \in L(X)$ we define the set of successors (respectively, predecessors) of w in X by

$$\mathrm{succ}_X(w) = \{a \in A \mid wa \in L(X)\}, \quad \mathrm{pred}_X(w) = \{a \in A \mid aw \in L(X)\}.$$

The notions of successors and predecessors are extended to one-way infinite sequences. For $x \in X$ we define

$$\begin{aligned} \mathrm{succ}_X(x[-\infty, 0]) &= \bigcap_{n \in \mathbb{N}} \mathrm{succ}_X(x[-n, 0]) \\ \mathrm{pred}_X(x[0, \infty]) &= \bigcap_{n \in \mathbb{N}} \mathrm{pred}_X(x[0, n]). \end{aligned}$$

Definition 2.3.8. Let $X \subseteq A^{\mathbb{Z}}$ and $Y \subseteq B^{\mathbb{Z}}$ be subshifts. We say that the map $F : X \to Y$ is a *sliding block code* from X to Y if there exist integers $m \leq a$ (memory and anticipation) and a *local rule* $f : A^{a-m+1} \to B$ such that $F(x)[i] = f(x[i+m], \ldots, x[i], \ldots, x[i+a])$. The quantity $d = a - m$ is the *diameter* of the local rule f. If $X = Y$, we say that F is a *cellular automaton* (CA). If we can choose f so that $-m = a = r \geq 0$, we say that F is a radius-r CA and if we can choose $m = 0$ we say that F is a *one-sided* CA. A one-sided CA with anticipation 1 is called a radius-$\frac{1}{2}$ CA.

We can extend any local rule $f : A^{d+1} \to B$ to words $w = w[1] \cdots w[d+n] \in A^{d+n}$ with $n \in \mathbb{N}_+$ by $f(w) = u = u[1] \cdots u[n]$, where $u[i] = f(w[i], \ldots, w[i+d])$.

The following observation can be found in [24].

Theorem 2.3.9 (Curtis-Hedlund-Lyndon)**.** A map $F : X \to Y$ between subshifts X and Y is a morphism between dynamical systems (X, σ) and (Y, σ) if and only if it is a sliding block code.

From this it follows in particular that if X is a subshift, then $\mathrm{End}(X)$ is the set of CA on X and $\mathrm{Aut}(X)$ is the set of reversible CA on X. Hedlund's theorem allows us to construct cellular automata $F : X \to X$ without explicitly giving any local rule: it is sufficient to define F so that it is continuous and that it commutes with $\sigma : X \to X$.

Remark 2.3.10. Technically it does not make any difference whether an element $F \in \mathrm{End}(X)$ is called a cellular automaton or an endomorphism when X is a subshift. In this thesis we will make a distinction based on the *role* the map F plays in a given context. If we think of F as forming a dynamical system (X, F), i.e. we are interested in repeated iteration of the map F on the points of X, then we say that F is a cellular automaton. If on the other hand it is natural to think of F as an element of $\mathrm{End}(X)$, e.g. if we are interested in the totality of the action of some larger monoid $\mathcal{M} \subseteq \mathrm{End}(X)$ containing F, then we say that F is an endomorphism. In a similar way we determine whether $F \in \mathrm{Aut}(X)$ is called a reversible CA or an automorphism.

For a given CA $F : X \to X$ and a configuration $x \in X$ it is often helpful to consider the *space-time diagram* of x with respect to F. Formally it is the map $\theta \in A^{\mathbb{Z}\times(-\mathbb{N})}$ (or possibly $\theta \in A^{\mathbb{Z}^2}$ when F is reversible) defined by $\theta(i, -j) = F^j(x)[i]$: the minus sign in this definition signifies that time increases in the negative direction of the vertical coordinate axis. Informally the space-time diagram of x is a picture which depicts elements of the sequence $(F^i(x))_{i\in\mathbb{N}}$ (or possibly $(F^i(x))_{i\in\mathbb{Z}}$ in the case when F is reversible) in such a way that $F^{i+1}(x)$ is drawn below $F^i(x)$ for every i. As an example, Figure 2.2 contains the space-time diagram of $x = \cdots 01101001 \cdots$ with respect to $\sigma : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$.

x	$\cdots$	0	1	1	0	1	0	0	1	$\cdots$
$\sigma(x)$	$\cdots$	1	1	0	1	0	0	1		$\cdots$
$\sigma^2(x)$	$\cdots$	1	0	1	0	0	1			$\cdots$

Figure 2.2: An example of a space-time diagram.

For a subshift $X \subseteq A^{\mathbb{Z}}$, a reversible CA $F : X \to X$, a configuration $x \in X$ and a nonempty interval $I = [i, j] \subseteq \mathbb{Z}$, the *I-trace* of x (with respect to F) is the configuration $\mathrm{Tr}_{F,I}(x)$ over the alphabet $A^{|I|}$ defined by

$$\mathrm{Tr}_{F,I}(x)[t] = (F^t(x)[i], F^t(x)[i+1], \ldots, F^t(x)[j]) \text{ for } t \in \mathbb{Z}.$$

If F is not reversible, $\mathrm{Tr}_{F,I}(x)$ can be similarly defined as an element of $(A^{|I|})^{\mathbb{N}}$. If $I = i$ is the degenerate interval, we may write $\mathrm{Tr}_{F,i}(x)$ and if $i = 0$, we may write $\mathrm{Tr}_F(x)$. If the CA F is clear from the context, we may write $\mathrm{Tr}_I(x)$. The *I-trace subshift of* F is defined by

$$\Xi_I(F) = \mathrm{Tr}_{F,I}(X) \subseteq (A^{|I|})^{\mathbb{Z}},$$

This is indeed a subshift. Namely, $\Xi_I(F)$ is closed in $(A^{|I|})^{\mathbb{Z}}$ as the image of the compact set X under the continuous map $\mathrm{Tr}_{F,I}$. It is also closed under

σ, because any $z \in \Xi_I(F)$ has a preimage $x \in X$ and then the image of $F(x)$ by $\mathrm{Tr}_{F,I}$ is $\sigma(z)$. This argument also shows that $\mathrm{Tr}_{F,I} : (X, F) \to (\Xi_I(F), \sigma)$ is a factor map. We may omit the subscript if $I = \{0\}$, i.e. $\Xi(F) = \Xi_{\{0\}}(F)$.

The trace subshifts of F form a universal collection of subshift factors of the dynamical systems (X, F) in the sense that any factor map $\psi : (X, F) \to (Z, \sigma)$ factors through a trace subshift, i.e. there is an interval $I \subseteq \mathbb{Z}$ and a factor map $\psi' : (\Xi_I(F), \sigma) \to (Z, \sigma)$ such that $\psi = \mathrm{Tr}_{F,I} \circ \psi'$.

Occasionally we consider cellular automata from the measure theoretical point of view. For a subshift X we denote by $\Sigma(\mathcal{C}_X)$ the *sigma-algebra* generated by the collection of cylinders $\mathcal{C}_X$. It is the smallest collection of subsets of X which contains all the elements of $\mathcal{C}_X$ and which is closed under complement and countable unions. A *measure* on X is a countably additive function $\mu : \Sigma(\mathcal{C}_X) \to [0, 1]$ such that $\mu(X) = 1$, i.e. $\mu(\bigcup_{i=0}^{\infty} A_i) = \sum_{i=0}^{\infty} \mu(A_i)$ whenever all $A_i \in \Sigma(\mathcal{C}_X)$ are pairwise disjoint. A measure μ on X is completely determined by its values on cylinders. We say that a cellular automaton $F : X \to X$ is *measure preserving* (with respect to a measure μ) if $\mu(F^{-1}(S)) = \mu(S)$ for all $S \in \Sigma(\mathcal{C})$.

The following definitions are ways to formalize what it means for a CA to thoroughly mix the points in a given subshift.

Definition 2.3.11. A measure preserving CA $F : X \to X$ is *ergodic* (with respect to a measure μ) if for every $S \in \Sigma(\mathcal{C})$ with $F^{-1}(S) = S$ either $\mu(S) = 0$ or $\mu(S) = 1$.

Definition 2.3.12. A measure preserving CA $F : X \to X$ (with respect to a measure μ) is *strongly mixing* (with respect to the same measure) if

$$\lim_{t \to \infty} \mu(F^{-t}(U) \cap V) = \mu(U)\mu(V)$$

for every $U, V \in \Sigma(\mathcal{C})$.

Strongly mixingness is a stronger notion than ergodicity. Namely, if $F : X \to X$ is strongly mixing and if $S \in \Sigma(\mathcal{C})$ is such that $F^{-1}(S) = S$, then

$$\mu(S) = \lim_{t \to \infty} \mu(F^{-t}(S) \cap S) = \mu(S)\mu(S),$$

which means that $\mu(S) = 0$ or $\mu(S) = 1$.

On full shifts $A^{\mathbb{Z}}$ we are mostly interested in the *uniform measure* determined by $\mu(\mathrm{Cyl}(w, i)) = |A|^{-|w|}$ for $w \in A^+$ and $i \in \mathbb{Z}$. By Theorem 5.4 in [24] any surjective CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ preserves this measure. For more on measure theory of cellular automata, see [46].

2.4 Notions of Complexity for Cellular Automata

The Devaney definition of chaos does not capture correctly what it means for the dynamics of a cellular automaton to be complex. If we consider for example the shift map $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$, then it is easy to verify that the dynamical system $(A^{\mathbb{Z}}, \sigma)$ is chaotic in the sense of Devaney, but this feels wrong by comparison with a typical space-time diagram with respect to σ (e.g. Figure 1.5), because the way the configuration evolves under repeated application of σ seems very straightforward. The notion of sensitivity is refined by Sablik's framework of directional dynamics [51].

Definition 2.4.1. Let $F : X \to X$ be a cellular automaton and let $p, q \in \mathbb{Z}$ be coprime integers, $q > 0$. Then p/q is a *sensitive direction* of F if $\sigma^p \circ F^q$ is sensitive. Similarly, p/q is an *almost equicontinuous direction* of F if $\sigma^p \circ F^q$ is almost equicontinuous.

Under this definition we see that $-1 = (-1)/1$ is an almost equicontinuous direction of $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ because $\sigma^{-1} \circ \sigma = \mathrm{Id}$ is equicontinuous. This is directly visible in the space-time diagram of Figure 1.5, because it looks like the space-time diagram of the identity map when it is followed along the red line. Note that the slope of the red line is equal to -1 with respect to the vertical axis extending downwards in the diagram.

Since almost equicontinuity is a notion of stability for dynamical systems, it seems that if we want to search for dynamically complex CA $F \in \mathrm{End}(X)$, we should at least require that F *has no almost equicontinuous directions.* By Proposition 2.1 of [51] it follows that if $F : X \to X$ is a CA and X is a transitive subshift, then any direction p/q is either sensitive or almost equicontinuous, in which case our requirement would be that all directions of F are sensitive.

Almost equicontinuity has an alternative characterization for cellular automata on transitive subshifts using blocking words.

Definition 2.4.2. Let $F : X \to X$ be a radius-r CA and $w \in L(X)$. We say that w is a *blocking word* if there is an integer e with $|w| \geq e \geq r + 1$ and an integer $p \in [0, |w| - e]$ such that

$$\forall x, y \in \mathrm{Cyl}_X(w, 0), \forall n \in \mathbb{N}, F^n(x)[p, p + e - 1] = F^n(y)[p, p + e - 1].$$

The following is proved in Proposition 2.1 of [51].

Proposition 2.4.3. If X is a transitive subshift and $F : X \to X$ is a CA, then F is almost equicontinuous if and only if it has a blocking word.

If a CA $F : X \to X$ is sensitive, it means that it is possible to make changes to an arbitrary configuration $x \in X$ arbitrarily far from the origin in such a way that the changes propagate to the neighborhood of the origin after applying the map F sufficiently many times. One way to quantify the complexity of a cellular automaton are its Lyapunov exponents, which tell how *quickly* changes made to a configuration can propagate in different directions under applying a given CA. The concept of Lyapunov exponents originally comes from the theory of differentiable dynamical systems, and the discrete variant of Lyapunov exponents for CA is from [55, 57]. For a fixed subshift $X \subseteq A^{\mathbb{Z}}$ and for $x \in X$, $s \in \mathbb{Z}$, denote $W_s^+(x) = \{y \in X \mid y[s,\infty] = x[s,\infty]\}$ and $W_s^-(x) = \{y \in X \mid y[-\infty,s] = x[-\infty,s]\}$. Then for given cellular automaton $F : X \to X$, $x \in X$, $n \in \mathbb{N}$, define

$$\Lambda_n^+(x,F) = \min\{s \geq 0 \mid \forall 1 \leq i \leq n : F^i(W_{-s}^+(x)) \subseteq W_0^+(F^i(x))\}$$
$$\Lambda_n^-(x,F) = \min\{s \geq 0 \mid \forall 1 \leq i \leq n : F^i(W_s^-(x)) \subseteq W_0^-(F^i(x))\}.$$

These have shift-invariant versions $\overline{\Lambda}_n^{\pm}(x,F) = \max_{i\in\mathbb{Z}} \Lambda_n^{\pm}(\sigma^i(x),F)$. The quantities

$$\lambda^+(x,F) = \lim_{n\to\infty} \frac{\overline{\Lambda}_n^+(x,F)}{n}, \qquad \lambda^-(x,F) = \lim_{n\to\infty} \frac{\overline{\Lambda}_n^-(x,F)}{n}$$

are called (when the limits exist) respectively the right and left *Lyapunov exponents of* x (with respect to F).

A global version of these are the quantities

$$\lambda^+(F) = \lim_{n\to\infty} \max_{x\in X} \frac{\Lambda_n^+(x,F)}{n}, \qquad \lambda^-(F) = \lim_{n\to\infty} \max_{x\in X} \frac{\Lambda_n^-(x,F)}{n}$$

that are called respectively the right and left *Lyapunov exponents of* F. These limits exist by an application of Fekete's subadditive lemma (e.g. Lemma 4.1.7 in [43]).

Measure theoretical variants of these quantities are defined as follows. Given a measure μ on X and for $n \in \mathbb{N}$, let $I_{n,\mu}^+(F) = \int_{x\in X} \Lambda_n^+(x,F)d\mu$ and $I_{n,\mu}^-(F) = \int_{x\in X} \Lambda_n^-(x,F)d\mu$. Then the quantities

$$I_\mu^+(F) = \liminf_{n\to\infty} \frac{I_{n,\mu}^+(F)}{n}, \qquad I_\mu^-(F) = \liminf_{n\to\infty} \frac{I_{n,\mu}^-(F)}{n}$$

are called respectively the right and left *average Lyapunov exponents of* F (with respect to the measure μ).

We will write $W_s^{\pm}(x)$, $\Lambda_n^{\pm}(x)$, $\lambda^+(x)$, $I_{n,\mu}^+$ and I_μ^+ when X and F are clear by the context.

Kůrka suggested a language theoretical classification for cellular automata. The following definition was given in [41] for general dynamical systems on zero-dimensional spaces.

Definition 2.4.4. A cellular automaton $F : X \to X$ is *regular* if all its subshift factors are sofic shifts.

This definition is motivated in [40]. Taking a subshift factor Y of $F : X \to X$ corresponds to taking a finite (clopen) partition $\{X_1, \ldots, X_n\}$ of X, an "observation window", and observing for each $x \in X$ the infinite sequence of partition elements visited by x under repeated application of the map F. Regularity of F means that the totality of all sequences of observations form a "simple" set Y for arbitrarily precise observation windows. On the other hand, non-regularity means that F has complex behavior that can be detected by a suitable partition of X. Since the trace subshifts of F form a universal collection of subshift factors for (X, F), to test the regularity of F it is sufficient to test the soficness of the trace subshifts. Non-regularity is mostly an interesting notion of complexity for cellular automata acting on sofic shifts, because e.g. the shift map $\sigma : X \to X$ is non-regular whenever X is not a sofic shift.

Chapter 3

Multiplication Automata

In this chapter we focus on multiplication automata, which perform multiplication by nonnegative numbers in some integer base. The cellular automata in this class are (with some exceptions) weak universal pattern generators, i.e. they eventually generate all finite sequences when initialized on any finite nontrivial configuration. We consider this property as one possible yardstick of complex behavior. We hope that further study will eventually allow us to construct other classes of cellular automata that have the universal pattern generation property. With this goal in mind, we will present a broad case study of multiplication automata from the point of view of symbolic, topological and measurable dynamics. We will also present applications to a number theoretical problem presented by Mahler [45].

3.1 The Definition of Multiplication Automata and Universal Pattern Generators

In this section we give a natural definition of what it means for a cellular automaton to perform multiplication by nonnegative numbers. On one-sided configuration spaces all such automata were characterized in [4] and from this the characterization of all multiplication automata would also follow for the two-sided configuration spaces $\Sigma_n^{\mathbb{Z}}$. We present the construction and characterization of such automata on $\Sigma_n^{\mathbb{Z}}$ with proofs for the sake of completeness.

Recall that $\Sigma_n = \{0, 1, \dots, n-1\}$ for $n \in \mathbb{N}$, $n > 1$. To perform multiplication using a CA we need be able to represent a nonnegative real number as a configuration in $\Sigma_n^{\mathbb{Z}}$. If $\xi \geq 0$ is a real number and $\xi = \sum_{i=-\infty}^{\infty} \xi_i n^i$ is the unique base-n expansion of ξ such that $\xi_i \neq n-1$ for infinitely many $i < 0$, we define $\mathrm{config}_n(\xi) \in \Sigma_n^{\mathbb{Z}}$ by

$$\mathrm{config}_n(\xi)[i] = \xi_{-i}$$

for all $i \in \mathbb{Z}$. In reverse, whenever $x \in \Sigma_n^{\mathbb{Z}}$ is such that $x[i] = 0$ for all sufficiently small i, we define

$$\mathrm{real}_n(x) = \sum_{i=-\infty}^{\infty} x[-i]n^i.$$

For words $w = w[1]w[2]\cdots w[k] \in \Sigma_n^k$ we define analogously

$$\mathrm{real}_n(w) = \sum_{i=1}^{k} w[i]n^{-i}.$$

Clearly $\mathrm{real}_n(\mathrm{config}_n(\xi)) = \xi$ and $\mathrm{config}_n(\mathrm{real}_n(x)) = x$ for every $\xi \geq 0$ and every $x \in \Sigma_n^{\mathbb{Z}}$ such that $x[i] = 0$ for all sufficiently small i and $x[i] \neq n-1$ for infinitely many $i > 0$.

The fractional part of a number $\xi \in \mathbb{R}$ is

$$\mathrm{frac}(\xi) = \xi - \lfloor \xi \rfloor \in [0, 1).$$

Definition 3.1.1. For $\alpha \in \mathbb{R}_{>0}$ and a natural number $n \geq 2$, we denote by $\Pi_{\alpha,n} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ the cellular automaton such that

$$\mathrm{real}(\Pi_{\alpha,n}(x)) = \alpha\,\mathrm{real}(x)$$

for every finite configuration $x \in \Sigma_n^{\mathbb{Z}}$, whenever such an automaton exists. We say that $\Pi_{\alpha,n}$ multiplies by α in base n.

The cellular automaton of this definition is unique whenever it exists. Namely, let F and F' be CA that satisfy the assumption for some α, n. The function $\mathrm{real} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ is clearly injective on the set of finite configurations, so the values of F and F' are determined on the dense set of finite configurations. Since F and F' are continuous functions that agree on a dense set, it follows that $F = F'$.

For integers $p, n \geq 2$ where p divides n let $g_{p,n} : \Sigma_n \times \Sigma_n \to \Sigma_n$ be defined as follows. Let q be such that $pq = n$. Digits $a, b \in \Sigma_{pq}$ are represented as $a = a_1 q + a_0$ and $b = b_1 q + b_0$, where $a_0, b_0 \in \Sigma_q$ and $a_1, b_1 \in \Sigma_p$: such representations always exist and they are unique. Then

$$g_{p,n}(a, b) = g_{p,n}(a_1 q + a_0, b_1 q + b_0) = a_0 p + b_1.$$

An example in the particular case $(p, n) = (3, 6)$ is given in Figure 3.1.

We define the CA $\Pi_{p,n} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ by $\Pi_{p,n}(x)[i] = g_{p,n}(x[i], x[i+1])$, so $\Pi_{p,n}$ has memory 0 and anticipation 1. Giving the name $\Pi_{p,n}$ to this CA is in agreement with Definition 3.1.1 by the following lemma.

Lemma 3.1.2. $\mathrm{real}_n(\Pi_{p,n}(\mathrm{config}_n(\xi))) = p\xi$ for all $\xi \geq 0$.

$a\backslash b$	0	1	2	3	4	5
0	0	0	1	1	2	2
1	3	3	4	4	5	5
2	0	0	1	1	2	2
3	3	3	4	4	5	5
4	0	0	1	1	2	2
5	3	3	4	4	5	5

Figure 3.1: The values of $g_{3,6}(a,b)$.

Proof. Let $x = \mathrm{config}_n(\xi)$. Let $pq = n$ and for every $i \in \mathbb{Z}$, denote by $x[i]_0$ and $x[i]_1$ the natural numbers such that $0 \leq x[i]_0 < q$, $0 \leq x[i]_1 < p$ and $x[i] = x[i]_1 q + x[i]_0$. Then

$$\begin{aligned}
&\mathrm{real}_n(\Pi_{p,n}(\mathrm{config}_n(\xi))) = \mathrm{real}_n(\Pi_{p,n}(x)) = \sum_{i=-\infty}^{\infty} \Pi_{p,n}(x)[-i](pq)^i \\
&= \sum_{i=-\infty}^{\infty} g_{p,n}(x[-i], x[-i+1])(pq)^i = \sum_{i=-\infty}^{\infty} (x[-i]_0 p + x[-i+1]_1)(pq)^i \\
&= \sum_{i=-\infty}^{\infty} (x[-i]_0 p(pq)^i + x[-i+1]_1 pq(pq)^{i-1}) \\
&= \sum_{i=-\infty}^{\infty} (x[-i]_0 p(pq)^i + x[-i]_1 pq(pq)^i) \\
&= p \sum_{i=-\infty}^{\infty} (x[-i]_1 q + x[-i]_0)(pq)^i = p\,\mathrm{real}_{pq}(x) = p\,\mathrm{real}_{pq}(\mathrm{config}_{pq}(\xi)) = p\xi.
\end{aligned}$$

□

We have now seen that the CA $\Pi_{p,n}$ and $\Pi_{q,n}$ exist when $p, q \in \mathbb{N}$ are such that $pq = n$. We show that in this case $\Pi_{p,n}$ is reversible. Indeed, if $x \in \Sigma_n^{\mathbb{Z}}$ is a configuration with a finite number of non-zero coordinates, then

$$\begin{aligned}
&\Pi_{q,n}(\Pi_{p,n}(x)) = \Pi_{q,n}(\Pi_{p,n}(\mathrm{config}_{pq}(\mathrm{real}_{pq}(x)))) \\
&\overset{L3.1.2}{=} \Pi_{q,n}(\mathrm{config}_{pq}(p\,\mathrm{real}_{pq}(x))) \overset{L3.1.2}{=} \mathrm{config}_{pq}((pq\,\mathrm{real}_{pq}(x)) = \sigma(x).
\end{aligned}$$

Since $\sigma^{-1} \circ \Pi_{q,n} \circ \Pi_{p,n}$ is continuous and agrees with the identity function on a dense set, it follows that $\sigma^{-1}(\Pi_{q,n}(\Pi_{p,n}(x))) = x$ for all configurations $x \in \Sigma_{pq}^{\mathbb{Z}}$. Similarly $\Pi_{p,n}(\sigma^{-1}(\Pi_{q,n}(x))) = x$ for $x \in \Sigma_{pq}^{\mathbb{Z}}$. Thus $\sigma^{-1}(\Pi_{q,n}(x))$ is the inverse of $\Pi_{p,n}$ and it must be equal to $\Pi_{1/p,n}$.

Whenever $\alpha = p/q$ where p and q are products of prime factors p_i' and q_i' of n, one can define $\Pi_{\alpha,n}$ as a corresponding product of $\Pi_{p_i',n}$ and $\Pi_{1/q_i',n}$. It is shown in [4] that these are all the CA that multiply by positive reals in base n.

Theorem 3.1.3 (Blanchard, Host, Maass [4])**.** The multiplication automaton $\Pi_{\alpha,n} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ exists precisely when $\alpha = p/q$ where p and q are products of prime factors of n.

We recall the notion of universal pattern generators from [32].

Definition 3.1.4. A cellular automaton $F : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ together with a finite configuration $x \in \Sigma_n^{\mathbb{Z}}$ are a *weak universal pattern generator* if for every $w \in \Sigma_n^+$ there is a $t \in \mathbb{N}$ such that w occurs in $F^t(x)$. They are a *strong universal pattern generator* if for every $w \in \Sigma_n^+$ and every $i \in \mathbb{Z}$ there is a $t \in \mathbb{N}$ such that w occurs in $F^t(x)$ at position i.

The existence of such automata was questioned by Ulam on page 30 of [58]: "Assuming that at time t only a finite set of points are active, one wants to know how the activation will spread. In particular, do there exist "universal" systems which are capable of generating arbitrary systems of states?"

It is noted in [32, 33] that $\Pi_{3,6}$ together with any finite configuration $x \neq 0^{\mathbb{Z}}$ is a weak universal pattern generator. The argument is non-combinatorial in the sense that it relies on the irrationality of the number $\log_6 3$. By imitating this argument it is not difficult to completely characterize all multiplication automata that are weak universal pattern generators. We will give this characterization for the sake of completeness. The fact that these automata are weak universal pattern generators also together with all *aperiodic* (not necessarily finite) configurations was proved by Hartman [23] using Furstenberg's theorem [6, 11, 20]. Hartman's result would also follow from a result of Berend [2] by relating the automata $\Pi_{\alpha,n}$ to multiplication by α on the n-solenoid instead of multiplication by α on $\mathbb{R}_{\geq 0}$.

Definition 3.1.5. Natural numbers $p, q > 1$ are *multiplicatively independent* if $\log p/\log q$ is irrational. Otherwise they are *multiplicatively dependent.*

Lemma 3.1.6. Let $p, q > 1$ be natural numbers that are products of prime factors of $n > 1$.

1. If p and q are coprime then for sufficiently large $k \in \mathbb{N}$, $\frac{p}{q}n^k$ is a natural number which is multiplicatively independent with n.

2. If q and n are multiplicatively independent then for sufficiently large $k \in \mathbb{N}$, $\frac{n^k}{q}$ is a natural number which is multiplicatively independent with n.

Proof. For the first statement, note that $\frac{p}{q}n^k$ is a natural number greater than 1 for some $k \in \mathbb{N}$, because q is a product of prime factors of n. To prove multiplicative independence, assume to the contrary that $\log \frac{p}{q}n^k/\log n = i/j$ for some $i, j \in \mathbb{N}_+$. This is equivalent to the statement that $p^j n^{jk} = q^j n^i$.

If $jk \geq i$, then both sides of the equation $p^j n^{jk-i} = q^j$ are integers. This is not possible because p and q are coprime and therefore p on the left hand side cannot divide q^j on the right hand side. We reach a similar contradiction in the case $jk \leq i$.

For the second statement, note that $\frac{n^k}{q}$ is a natural number greater than 1 for some $k \in \mathbb{N}$, because q is a product of prime factors of n. To prove multiplicative independence, note that $\log \frac{n^k}{q} / \log n = k - \log q / \log n$ is irrational, because by assumption q and n are multiplicatively independent. $\square$

Theorem 3.1.7. Let $n \geq 2$ and let $p, q \geq 2$ be products of prime factors of n. Let $x \in \Sigma_n^{\mathbb{Z}}$ be finite and $x \neq 0^{\mathbb{Z}}$. If

1. p and n are multiplicatively independent and $\beta \in \left\{p, \frac{1}{p}\right\}$ or
2. p and q are coprime and $\beta = \frac{p}{q}$, then

$\Pi_{\beta,n}$ and x are a universal pattern generator.

Proof. Assume first that we are considering a CA $\Pi_{\beta,n}$ where β is of the form $1/p$ or p/q. By Lemma 3.1.6 the cellular automaton $\Pi_{\beta,n} \circ \sigma^k$ multiplies by an integer that is multiplicatively independent with n whenever k is sufficiently large. The CA $\Pi_{\beta,n}$ is a universal pattern generator with x if and only if $\Pi_{\beta,n} \circ \sigma^k$ is, so it is sufficient to prove the result for $\Pi_{p,n}$ where p and n are multiplicatively independent.

Let $w = w[1]w[2] \cdots w[m] \in \Sigma_n^+$ be arbitrary. We need to show that w occurs as a subword in some configuration $\Pi_{p,n}^t(x)$ ($t \in \mathbb{N}$), or equivalently that $\sigma^i(\Pi_{p,n}^t(x)) \in \mathrm{Cyl}(w, 1)$ for some $i \in \mathbb{Z}$, $t \in \mathbb{N}$. Let $r \in \mathbb{R}_{\geq 0}$ be the number with base-n expansion $0.w[1]w[2] \cdots w[m]$ and $I = (r, r + n^{-m})$ an open interval.

By the definition of multiplicative independence the number $\log_n p$ is irrational and the set $\{\mathrm{frac}(t \log_n p) \mid t \in \mathbb{N}\}$ is dense on the unit interval. In particular there are integers $t \in \mathbb{N}$ and $m \in \mathbb{Z}$ such that $t \log_n(p) + m \in \log_n(I / \mathrm{real}_n(x))$, or equivalently that $p^t \cdot n^m \cdot \mathrm{real}_n(x) \in I$. Therefore the base-$n$ expansion of $p^t \cdot n^m \cdot \mathrm{real}_n(x)$ begins as $0.w\ldots$ and $\sigma^m(\Pi_{p,n}^t(x)) \in \mathrm{Cyl}(w, 1)$. $\square$

We complete the characterization by noting that other multiplication automata are roots of some shift map, from which it follows that they do not form weak universal pattern generators together with any finite configurations.

Theorem 3.1.8. Let $n \geq 2$ and let $p \geq 2$ be a product of prime factors of n. If n and p are multiplicatively dependent and $\beta \in \{p, \frac{1}{p}\}$, then there are $i \in \mathbb{N}_+$, $j \in \mathbb{Z}$ such that $\Pi_{\beta,n}^i = \sigma^j$. In particular $\Pi_{\beta,n}$ and x are not a universal pattern generator for any finite configuration $x \in \Sigma_n^{\mathbb{Z}}$.

Proof. By assumption $\log p/\log n$ is rational, i.e. $\log p/\log n = i/j$ and $p^i = n^j$ for some non-zero $i, j \in \mathbb{Z}$. Then $\Pi^i_{\beta,n}$ is equal to either σ^j or σ^{-j} depending on the value of β. Therefore, if $w \in \Sigma^+$ is a word which occurs in $\Pi^t_{\beta,n}$ for some $t \in \mathbb{N}$, then w occurs in $\Pi^t_{\beta,n}$ already for some $0 \leq t < i$. Clearly there are some words w for which this does not happen, so $\Pi_{\beta,n}$ and x are not a universal pattern generator. $\square$

The multiplication automata are the only known weak universal pattern generators. No strong universal pattern generators are known. The following two questions are from [32].

Problem 3.1.9. Does there exist a weak universal pattern generator over the binary alphabet Σ_2?

Problem 3.1.10. Do any strong universal pattern generators exist? For example, is the automaton $\Pi_{3/2,6}$ a strong universal pattern generator together with any finite configurations?

Recall that all multiplication automata are reversible. In light of this we ask the following.

Problem 3.1.11. Do any non-reversible universal pattern generators exist?

Wolfram's Rule 30 automaton $W_{30} : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$ is defined by

$$W_{30}(x)[i] = x[i-1] + x[i] + x[i+1] + x[i]x[i+1] \pmod 2$$

for all $x \in \Sigma_2^{\mathbb{Z}}$, see Figure 3.2. This is a surjective non-reversible CA and it is conjectured on page 725 of [61] that W_{30} together with the configuration containing a single occurrence of the digit 1 is a weak universal pattern generator over the binary alphabet. The strongest proven result concerning the seemingly random nature of W_{30} is the following.

Theorem 3.1.12 (Jen [28])**.** If $x \in \Sigma_2^{\mathbb{Z}}$ is a finite configuration not equal to $0^{\mathbb{Z}}$, then $\mathrm{Tr}_{W_{30},[0,1]}(x)$ (the trace of width 2), is not eventually periodic.

In Proposition 3.3.5 we prove an analogous result for a class of multiplication automata. It still seems to be an open problem whether $\mathrm{Tr}_{W_{30}}(x)$ (the trace of width 1) can be eventually periodic for some finite $x \neq 0^{\mathbb{Z}}$. We ask another question related to traces of W_{30}.

Problem 3.1.13. Is W_{30} regular?

In Corollary 3.4 we prove non-regularity of a class of multiplication automata.

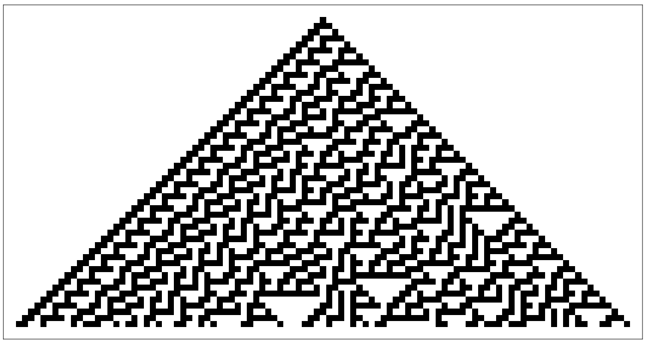

Figure 3.2: The space-time diagram of $\cdots 0001000 \cdots$ under $W_{30} : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$. White and black squares correspond to digits 0 and 1 respectively.

3.2 Characterizing the Class of Multiplication Automata

Multiplication automata $\Pi_{\alpha,n}$ do not exist for all $\alpha > 0$. This is due to the fact that all cellular automata are defined by local rules. Consider for example multiplication by 3 in base 10 and assume that the hypothetical CA $\Pi_{3,10}$ had radius $r \geq 1$. If $\xi_1 = 0.333\cdots 33 \in \mathbb{R}_{>0}$ and $\xi_2 = 0.333\cdots 34 \in \mathbb{R}_{>0}$ are numbers with r consecutive occurrences of the digit 3 in their base-10 representations, then $3 \cdot \xi_1 < 1$ and $1 < 3 \cdot \xi_2 < 2$, so the base-10 representations of $3 \cdot \xi_1$ and $3 \cdot \xi_2$ differ to the left of the decimal point, contradicting the assumption that the radius of $\Pi_{3,10}$ is r. This is the main idea behind the proof of Theorem 3.1.3 in [4].

We can give an interesting alternative proof of Theorem 3.1.3 when we restrict our attention to reversible CA. Our proof uses the fact that $\Pi_{p,n}$ are partitioned CA when p is a factor of n.

Definition 3.2.1. A *partial shift* on the alphabet $B \times C$ is a CA $\tau : (B \times C)^{\mathbb{Z}} \to (B \times C)^{\mathbb{Z}}$ defined by $\tau(x) = (\sigma(x_1), x_2)$ for all $x = (x_1, x_2)$ where $x_1 \in B^{\mathbb{Z}}$ and $x_2 \in C^{\mathbb{Z}}$. More generally, if $\pi : A \to B \times C$ is a bijection, then it is naturally extended to a bijective sliding block code $\pi : A^{\mathbb{Z}} \to (B \times C)^{\mathbb{Z}}$ and we call $\pi^{-1} \circ \tau \circ \pi : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ a partial shift on the alphabet A.

Definition 3.2.2. A CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a *partitioned CA* if $F = \rho \circ \tau$ where $\rho : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a coordinatewise symbol permutation and τ is a partial shift on A.

On the alphabets Σ_n consisting of digits we define a collection of canonical partial shifts. For any $p \in \mathbb{N}$ dividing n let $q \in \mathbb{N}$ such that $pq = n$. Then we can define the bijection $\pi : \Sigma_n \to \Sigma_p \times \Sigma_q$ by $\pi(a) = (a_1, a_0)$ where $a = a_1 q + a_0$ is the unique way to write $a \in \Sigma_n$ so that $a_1 \in \Sigma_p$ and $a_0 \in \Sigma_q$.

If τ is defined on $(\Sigma_p \times \Sigma_q)^{\mathbb{Z}}$ by $\tau(x_1, x_2) = (\sigma(x_1), x_2)$, we say that the map $\tau_p = \pi^{-1} \circ \tau \circ \pi : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ is *the canonical p-shift over n*.

It is now easily seen, as noted in [32], that under this definition $\Pi_{p,n} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ is a partitioned CA when p is a factor of n. Namely, if $q \in \mathbb{N}$ is such that $pq = n$ and if $\rho : \Sigma_{pq} \to \Sigma_{pq}$ is the map $\rho(a_1 q + a_0) = a_0 p + a_1$, we see by comparison to the definition of the local rule $g_{p,n}$ that $\Pi_{p,n} = \rho \circ \tau_p$.

We will use in our argument the group homomorphism $\delta : \mathrm{Aut}(\Sigma_n^{\mathbb{Z}}) \to \mathbb{R}_{>0}$ defined in [31]. For $F \in \mathrm{Aut}(\Sigma_n^{\mathbb{Z}})$ let $r > 0$ be a radius of both F and F^{-1}. The set of *left stairs* of F is

$$L_F = \{(x[-r, r-1], F(x)[0, 2r-1]) \mid x \in \Sigma_n^{\mathbb{Z}}\}$$

(the reason for calling these "stairs" is apparent by Figure 3.3) and we then define $\delta(F) = |L_F|/n^{3r}$. The non-trivial facts that $\delta(F)$ does not depend on the choice of r and that δ is indeed a group homomorphism are shown in [31]. This homomorphism is an instance of a more general construction known as the *dimension representation* which can be defined on $\mathrm{Aut}(X)$ for any SFT X, see. e.g. Section 6 in [10].

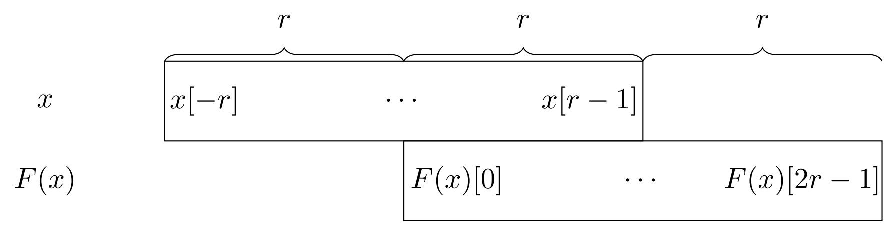

Figure 3.3: A left stair found in a space-time diagram.

We recall some basic properties of the map δ noted in [31]. It is easy to verify that $\delta(\sigma) = n$ for the shift $\sigma : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ and $\delta(\tau_p) = p$ for the p-shift over n. If F is a finite order automorphism, i.e. $F^t = \mathrm{Id}$ for some $t \in \mathbb{N}_+$, then $\delta(F) = 1$: this is due to the fact that 1 is the only finite order element in the multiplicative group $\mathbb{R}_{>0}$. From the definition of δ it follows that $\mathrm{Im}(\delta)$ is equal to the multiplicative subgroup of $\mathbb{R}_{>0}$ generated by $p_1, \dots, p_k$ where p_i are the prime factors of n.

Lemma 3.2.3. Let $p_1, \dots, p_k$ be the prime factors of n. For any $\alpha \in \mathrm{Im}(\delta)$ there is a multiplication automaton $\Pi_{\alpha,n}$ which is some product of multiplication automata $\Pi_{p_i,n}$ and their inverses and which satisfies $\delta(\Pi_{\alpha,n}) = \alpha$.

Proof. Since $\mathrm{Im}(\delta)$ is generated by the prime factors of n, it is sufficient to prove the lemma for $\alpha = p$ which is a prime factor of n. We have seen that $\Pi_{p,n} = \rho \circ \tau_p$ where ρ is a symbol permutation and in particular it is a finite order automorphism. Since δ is a homomorphism, it follows that $\delta(\Pi_{p,n}) = \delta(\rho)\delta(\tau_p) = 1 \cdot p = p$. $\square$

Lemma 3.2.4. If $\Pi_{\alpha,n}$ is in the kernel of $\delta : \mathrm{Aut}(\Sigma_n^{\mathbb{Z}}) \to \mathbb{R}_{>0}$, then $\alpha = 1$.

Proof. Assume to the contrary that $\alpha \neq 1$. We may assume without loss of generality that $\alpha > 1$ (by considering $\Pi_{\alpha,n}^{-1}$ instead of $\Pi_{\alpha,n}$ if necessary). Let r be a common radius of $\Pi_{\alpha,n}$ and its inverse. By our assumption $\delta(\Pi_{\alpha,n}) = 1$, so by the definition of δ the set $L = L_F$ should contain n^{3r} elements. We will find a contradiction by concretely enumerating the left stairs.

Let $u_i \in \Sigma_n^r$ $(0 \leq i < n^r)$ be an enumeration of elements of Σ_n^r and let $v_j \in \Sigma_n^{2r}$ $(0 \leq j < n^{2r})$ be an enumeration of elements of Σ_n^{2r}. For all such i, j define $y_{i,j} \in \Sigma_n^{\mathbb{Z}}$ by $y_{i,j}[-r, 2r-1] = u_i v_j$, $y_{i,j}[k] = 0$ for $k \notin [-r, 2r-1]$. Let $(w_{i,j}, v_j)$ be the left stair derived from the configuration $x_{i,j} = \Pi_{\alpha,n}^{-1}(y_{i,j})$, i.e. $w_{i,j} = x_{i,j}[-r, r-1]$ (and $v_j = y_{i,j}[0, 2r-1]$ by the definition of $y_{i,j}$).

We first show that all the left stairs of the form $(w_{i,j}, v_j)$ $(0 \leq i < n^r$, $0 \leq j < n^{2r})$ are distinct. Let i, i', j, j' be such that $(w_{i,j}, v_j) = (w_{i',j'}, v_{j'})$. From $v_j = v_{j'}$ it follows that $j = j'$ and it remains to show that $i = i'$. Since $\Pi_{\alpha,n}^{-1}$ has radius r, from $v_j = v_{j'}$ it follows that $x_{i,j}[r, \infty] = x_{i',j}[r, \infty]$. Since $\alpha > 0$, from $y_{i,j}[-\infty, -r-1] = y_{i',j}[-\infty, -r-1] = {}^{\infty}0$ it follows that $x_{i,j}[-\infty, -r-1] = x_{i',j}[-\infty, -r-1] = {}^{\infty}0$. Combining these observations with $w_{i,j} = w_{i',j}$ it follows that $x_{i,j} = x_{i',j}$. Applying $\Pi_{\alpha,n}$ to this equality we get $y_{i,j} = y_{i',j}$, so in particular $u_i = u_{i'}$ and $i = i'$.

We show that $w_{i,j} \neq (n-1)^{2r}$ for all choices of i and j. Assume to the contrary that $w_{i,j} = (n-1)^{2r}$ for some i, j. Consider the configuration $x' = 0^{\mathbb{Z}} \otimes_{-r} (n-1)^{\mathbb{Z}}$. Since $\alpha > 0$ and $\mathrm{real}_n(x') = n^{r+1}$, it follows that in the configuration $y' = \Pi_{\alpha,n}(x')$ we have $y'[k] \neq 0$ for some $k < -r$. Since $x_{i,j}[-\infty, r-1] = x'[-\infty, r-1]$ and $\Pi_{\alpha,n}$ has radius r, it follows that $y_{i,j}[-\infty, -1] = y'[-\infty, -1]$ and in particular $y_{i,j}[k] \neq 0$ for some $k < -r$. This contradicts the definition of $y_{i,j}$.

There exists a left stair of the form (w, v) where $w = (n-1)^{2r}$, and by the previous paragraph it is different from all the left stairs of the form $(w_{i,j}, v_j)$ $(0 \leq i < n^r$, $0 \leq j < n^{2r})$. It follows that $|L| \geq n^{3r} + 1$, contradicting the assumption $\delta(\Pi_{\alpha,n}) = 1$. $\square$

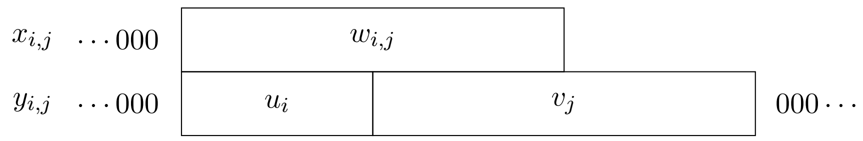

Figure 3.4: Left stairs of the form $(w_{i,j}, v_j)$.

Theorem 3.2.5. All the reversible multiplication automata over $\Sigma_n^{\mathbb{Z}}$ are precisely of the form $\Pi_{p/q,n}$ where p and q are products of prime factors of n.

Proof. We noted in the previous subsection that $\Pi_{p/q,n}$ exist whenever p and q are products of prime factors of n. To see the other direction, let $\Pi_{\alpha',n}$ be an arbitrary reversible multiplication automaton where $\alpha' \in \mathbb{R}_{>0}$. By Lemma 3.2.3 there is $\alpha = p/q$ where p and q are products of prime factors of n such that $\delta(\Pi_{\alpha,n}) = \delta(\Pi_{\alpha',n})$. Therefore $\delta(\Pi_{\alpha/\alpha',n}) = 1$ and $\alpha' = \alpha$ by Lemma 3.2.4. $\square$

Lemma 3.2.4 implies in particular that if a multiplication automaton $\Pi_{\alpha,n}$ is a weak universal pattern generator then $\delta(\Pi_{\alpha,n}) \neq 1$.

Problem 3.2.6. Does the kernel of $\delta : \mathrm{Aut}(\Sigma_n^{\mathbb{Z}}) \to \mathbb{R}_{>0}$ contain a weak universal pattern generator for any $n \geq 2$?

Since any reversible CA on $\Sigma_2^{\mathbb{Z}}$ can be represented as a composition $\sigma^k \circ F$ where F is in the kernel of $\delta : \mathrm{Aut}(\Sigma_2^{\mathbb{Z}}) \to \mathbb{R}_{>0}$ and $k \in \mathbb{Z}$, a negative answer to this question would imply a negative answer to Problem 3.1.9 when restricted to reversible CA.

3.3 The Basic Properties of Fractional Multiplication Automata

When $p, q \geq 2$ are coprime integers, the multiplication automata $\Pi_{p/q,pq}$ have particularly nice properties that can be derived directly by examining the local rules. In this section we mostly focus on such automata. We assume throughout this section that $p, q \geq 2$ are coprime.

Recall that the shift CA $\sigma : \Sigma_{pq}$ multiplies by pq in base pq and its inverse divides by pq. This combined with Lemma 3.1.2 shows that the CA $\Pi_{p/q,pq}$ multiplying by p/q in base pq can be constructed as the composition $\sigma^{-1} \circ \Pi_{p,pq} \circ \Pi_{p,pq}$. Earlier we explicitly defined local rules $g_{p,pq}$ for the automata $\Pi_{p,pq}$ which we can use to define local rules $f_{p/q,pq} : \Sigma_{pq}^3 \to \Sigma_{pq}$ also for the automata $\Pi_{p/q,pq}$ as follows:

$$\begin{aligned}\Pi_{p/q,pq}(x)[i] =& f_{p/q,pq}(x[i-1], x[i], x[i+1]) \\ \doteq& g_{p,pq}(g_{p,pq}(x[i-1], x[i]), g_{p,pq}(x[i], x[i+1]));\end{aligned}$$

the symbol f in $f_{p/q,pq}$ is used to emphasize the fact that this local rule is associated with multiplication by a *fraction*.

As an example, the local rule $f_{3/2,6}$ has been written out explicitly in Figure 3.5. We will prove some of the regularities seen in this figure for general $f_{p/q,pq}$.

By the construction of $\Pi_{p/q,pq}$, for every $x \in \Sigma_{pq}^{\mathbb{Z}}$ and every $i \in \mathbb{Z}$ the value of $\Pi_{p/q,pq}(x)[i]$ can be computed from $x[i-1], x[i]$ and $x[i+1]$, the three nearest digits above in the space-time diagram. Proposition 3.3.4 gives

$c = 0$

$a\backslash b$	0	1	2	3	4	5
0	0	0	0	0	1	1
1	3	3	3	3	4	4
2	0	0	0	0	1	1
3	3	3	3	3	4	4
4	0	0	0	0	1	1
5	3	3	3	3	4	4

$c = 1$

$a\backslash b$	0	1	2	3	4	5
0	1	1	2	2	2	2
1	4	4	5	5	5	5
2	1	1	2	2	2	2
3	4	4	5	5	5	5
4	1	1	2	2	2	2
5	4	4	5	5	5	5

$c = 2$

$a\backslash b$	0	1	2	3	4	5
0	3	3	3	3	4	4
1	0	0	0	0	1	1
2	3	3	3	3	4	4
3	0	0	0	0	1	1
4	3	3	3	3	4	4
5	0	0	0	0	1	1

$c = 3$

$a\backslash b$	0	1	2	3	4	5
0	4	4	5	5	5	5
1	1	1	2	2	2	2
2	4	4	5	5	5	5
3	1	1	2	2	2	2
4	4	4	5	5	5	5
5	1	1	2	2	2	2

$c = 4$

$a\backslash b$	0	1	2	3	4	5
0	0	0	0	0	1	1
1	3	3	3	3	4	4
2	0	0	0	0	1	1
3	3	3	3	3	4	4
4	0	0	0	0	1	1
5	3	3	3	3	4	4

$c = 5$

$a\backslash b$	0	1	2	3	4	5
0	1	1	2	2	2	2
1	4	4	5	5	5	5
2	1	1	2	2	2	2
3	4	4	5	5	5	5
4	1	1	2	2	2	2
5	4	4	5	5	5	5

Figure 3.5: The values of $f_{3/2,6}(a, c, b)$.

similarly that each digit in the space-time diagram can be computed from the three nearest digits to the right (see Figure 3.6). Its proof is broken down into the following sequence of lemmas.

Lemma 3.3.1. If $g_{p,pq}(a, c) = g_{p,pq}(b, d)$, then $a \equiv b \pmod q$.

Proof. Let $a = a_1q + a_0$, $b = b_1q + b_0$, $c = c_1q + c_0$ and $d = d_1q + d_0$. Then

$$\begin{aligned} g_{p,pq}(a, c) = g_{p,pq}(b, d) &\implies a_0p + c_1 = b_0p + d_1 \\ &\implies a_0 = b_0 \implies a \equiv b \pmod q. \end{aligned}$$

□

Lemma 3.3.2. $g_{p,pq}(a, c) \equiv g_{p,pq}(b, c) \pmod q \iff a \equiv b \pmod q \iff g_{p,pq}(a, c) = g_{p,pq}(b, c)$.

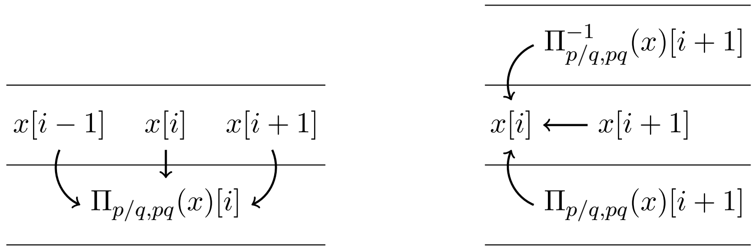

Figure 3.6: Determination of digits in the space-time diagram of x with respect to $\Pi_{p/q,pq}$.

Proof. Let $a = a_1q + a_0$, $b = b_1q + b_0$ and $c = c_1q + c_0$. Then

$$\begin{aligned} g_{p,pq}(a,c) \equiv g_{p,pq}(b,c) \pmod q &\iff a_0p + c_1 \equiv b_0p + c_1 \pmod q \\ &\iff a_0 = b_0 \iff a \equiv b \pmod q \end{aligned}$$

and

$$\begin{aligned} g_{p,pq}(a,c) = g_{p,pq}(b,c) &\iff a_0p + c_1 = b_0p + c_1 \\ &\iff a_0 = b_0 \iff a \equiv b \pmod q. \end{aligned}$$

□

These basic properties of $g_{p,pq}$ can be used to prove the following lemma concerning $f_{p/q,pq}$, because $f_{p/q,pq}$ was defined using $g_{p,pq}$. Similar reductions of $f_{p/q,pq}$ to $g_{p,pq}$ will be done also later.

Lemma 3.3.3. If $f_{p/q,pq}(a,c,d) = f_{p/q,pq}(b,c,e)$, then $a \equiv b \pmod q$.

Proof.

$$\begin{aligned} &f_{p/q,pq}(a,c,d) = f_{p/q,pq}(b,c,e) \\ \Longrightarrow\ &g_{p,pq}(g_{p,pq}(a,c), g_{p,pq}(c,d)) = g_{p,pq}(g_{p,pq}(b,c), g_{p,q}(c,e)) \\ \overset{L3.3.1}{\Longrightarrow}\ &g_{p,pq}(a,c) \equiv g_{p,pq}(b,c) \pmod q \overset{L3.3.2}{\Longrightarrow} a \equiv b \pmod q. \end{aligned}$$

□

Proposition 3.3.4. There is a radius-1 CA $\Delta_{p/q} : \Xi(\Pi_{p/q,pq}) \to \Xi(\Pi_{p/q,pq})$ such that $\Delta_{p/q}(\mathrm{Tr}_{\Pi_{p/q,pq},i}(x)) = \mathrm{Tr}_{\Pi_{p/q,pq},i-1}(x)$ for all $x \in \Sigma_{pq}^{\mathbb{Z}}$, $i \in \mathbb{Z}$.

Proof. Denote $y = \sigma^i(\Pi^k_{p/q,pq}(x))$. It suffices to show that $y[0]$ can be computed from $\Pi_{q/p,pq}(y)[1]$, $y[1]$ and $\Pi_{p/q,pq}(y)[1]$. Because $\Pi_{p/q,pq}(y)[1] = f_{p/q,pq}(y[0], y[1], y[2])$, by Lemma 3.3.3 the value of $y[0]$ modulo q can be computed from $y[1]$ and $\Pi_{p/q,pq}(y)[1]$ (see Figure 3.7, left). Similarly, because $\Pi_{q/p,pq}(y)[1] = f_{q/p,pq}(y[0], y[1], y[2])$, by the same lemma the value of $y[0]$ modulo p can be computed from $y[1]$ and $\Pi_{q/p,pq}(y)[1]$ (Figure 3.7, middle). In total, the value of $y[0]$ both modulo q and modulo p can be computed from $\Pi_{q/p,pq}(y)[1]$, $y[1]$ and $\Pi_{p/q,pq}(y)[1]$ (Figure 3.7, right). Because $y[0] \in \Sigma_{pq}$, this fully determines the value of $y[0]$. $\square$

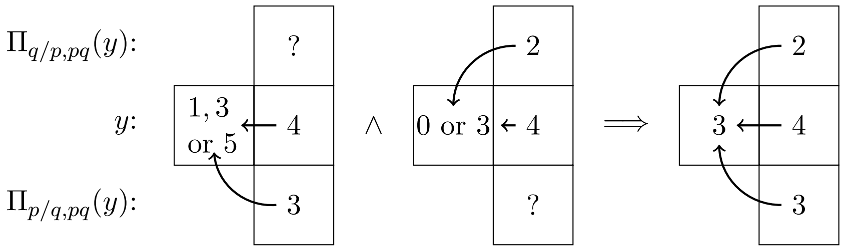

Figure 3.7: The proof of Proposition 3.3.4 (here $(p, n) = (3, 6)$).

As an application of this proposition we now prove a version of Theorem 3.1.12 for multiplication automata. The proof in [28] is based on the observations that digits in the space-time diagram of W_{30} are determined to the left in the sense similar to Proposition 3.3.4 and that all finite perturbations in the configuration $0^{\mathbb{Z}}$ must propagate to the left under the action of W_{30}. Our proof uses similar observations on $\Pi_{p/q,pq}$.

Proposition 3.3.5. Let $p > q$. If $x \in \Sigma_{pq}^{\mathbb{Z}}$ is a configuration that represents a positive real number (in particular, if x is a finite configuration different from $0^{\mathbb{Z}}$), then $\mathrm{Tr}_{\Pi_{p/q,pq}}(x)$ is not eventually periodic.

Proof. Let $x \in \Sigma_{pq}^{\mathbb{Z}}$ be such that $\mathrm{real}_{pq}(x) > 0$. Assume to the contrary that $y = \mathrm{Tr}_{\Pi_{p/q,pq}}(x)$ is eventually periodic, i.e. there are $P \in \mathbb{N}_+$, $i' \in \mathbb{N}$ such that $y[i + P] = y[i]$ for all $i \geq i'$, and we may assume that this holds even for all $i \in \mathbb{N}$ (by considering the configuration $\Pi_{p/q,pq}^{i'}(x)$ instead of x if necessary). Denote $x_t = (\sigma^{-1} \circ \Pi_{p/q,pq})^t(x)$ and $y_t = \mathrm{Tr}_{\Pi_{p/q,pq}}(x_t)$ for all $t \in \mathbb{N}$. An inductive application of Proposition 3.3.4 with respect to t shows that $y_t[i + P] = y_t[i]$ for all $i, t \in \mathbb{N}$.

Note that $\mathrm{real}_{pq}(x_t) = \left(\frac{1}{pq}\frac{p}{q}\right)^t \mathrm{real}_{pq}(x) = \mathrm{real}_{pq}(x)/q^{2t}$ for all $t \in \mathbb{N}$. Fix T so that $\left(\frac{p}{q}\right)^P \mathrm{real}_{pq}(x_T) < 1$. From this it follows that $y_T[-\infty, P] = {}^{\infty}0$ and by the eventual periodicity of y_T it follows that $y_T = 0^{\mathbb{Z}}$. Applying Proposition 3.3.4 shows that $y_t = 0^{\mathbb{Z}}$ for all $t \geq T$. In particular $\Pi_{p/q,pq}^t(x)[-\infty, -T] = {}^{\infty}0$ for $t \in \mathbb{N}$ and the sequence $\left(\left(\frac{p}{q}\right)^t \mathrm{real}_{pq}(x)\right)_{t \in \mathbb{N}}$ is bounded from above by $(pq)^T$, which contradicts the assumption that $\mathrm{real}_{pq}(x) > 0$. $\square$

An important class of CA on full shifts are the *permutive* cellular automata. We say that a CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ defined by a local rule $f : A^{d+1} \to A^{d+1}$ is left permutive if for every $w \in A^d$ it holds that $f(a, w) \neq f(b, w)$ whenever $a, b \in A$ are distinct (similarly one defines right permutive CA). This is equivalent to saying that the map $A \to A$ defined by $a \to f(a, w)$ is a permutation for every $w \in A^d$. The following lemma shows that $f_{p/q,pq}$ has a kind of a *partial* permutivity property: as the symbol a varies modulo q, also $f_{p/q,pq}(a, w)$ varies modulo q.

Lemma 3.3.6. $f_{p/q,pq}(a, c, d) \equiv f_{p/q,pq}(b, c, d) \pmod q$
$\iff a \equiv b \pmod q \iff f_{p/q,pq}(a, c, d) = f_{p/q,pq}(b, c, d)$.

Proof.

$$\begin{aligned}
& f_{p/q,pq}(a, c, d) \equiv f_{p/q,pq}(b, c, d) \pmod q \\
\iff & g_{p,pq}(g_{p,pq}(a, c), g_{p,pq}(c, d)) \equiv g_{p,pq}(g_{p,pq}(b, c), g_{p,pq}(c, d)) \pmod q \\
\overset{L3.3.2}{\iff} & g_{p,pq}(a, c) \equiv g_{p,pq}(b, c) \pmod q \overset{L3.3.2}{\iff} a \equiv b \pmod q \\
\overset{L3.3.2}{\iff} & g_{p,pq}(g_{p,pq}(a, c), g_{p,pq}(c, d)) = g_{p,pq}(g_{p,pq}(b, c), g_{p,pq}(c, d)) \\
\iff & f_{p/q,pq}(a, c, d) = f_{p/q,pq}(b, c, d)
\end{aligned}$$

□

Corollary 3.3.7. If $f_{p/q,pq}(a, c, d) = f_{p/q,pq}(b, c, e)$, then $f_{p/q,pq}(a, c, d) = f_{p/q,pq}(a, c, e)$.

Proof. By Lemma 3.3.3 $a \equiv b \pmod q$, so

$$f_{p/q,pq}(a, c, d) = f_{p/q,pq}(b, c, e) \overset{L3.3.6}{=} f_{p/q,pq}(a, c, e).$$

□

On the other hand, we show that as the symbol a varies modulo q, the value of $f_{p/q,pq}(a, w)$ remains constant modulo p. This is proved by reduction to $g_{p,pq}$.

Lemma 3.3.8. $g_{p,pq}(a, c) \equiv g_{p,pq}(b, c) \pmod p$.

Proof. Let $a = a_1 q + a_0$, $b = b_1 q + b_0$ and $c = c_1 q + c_0$. Then

$$g_{p,pq}(a, c) = a_0 p + c_1 \equiv b_0 p + c_1 = g_{p,pq}(b, c) \pmod p.$$

□

Lemma 3.3.9. $f_{p/q,pq}(a, c, d) \equiv f_{p/q,pq}(b, c, d) \pmod p$.

Proof.

$$f_{p/q,pq}(a,c,d) = g_{p,pq}(g_{p,pq}(a,c), g_{p,pq}(c,d))$$
$$\overset{L3.3.8}{\equiv} g_{p,pq}(g_{p,pq}(b,c), g_{p,pq}(c,d)) = f_{p/q,pq}(b,c,d) \pmod{p}.$$

□

For any $a \in \Sigma_{pq}$ denote

$$Q_{p,q}(a) = \{d \in \Sigma_{pq} \mid d \equiv a \pmod{p}\}.$$

The set $Q_{p,q}(a)$ contains q elements, all non-congruent modulo q. In particular $Q_{p,q}(a)$ is a complete residue system modulo q.

Proposition 3.3.10. Let $Q \subseteq \Sigma_{pq}$ contain a complete residue system modulo q and let $w \in \Sigma_{pq}^*$ be such that $|w| \geq 2$. Then

$$f_{p/q,pq}(Qw) = Q_{p,q}(b)w'$$

for some $b \in \Sigma_{pq}$ and $w' \in \Sigma_{pq}^*$, $|w'| = |w| - 2$. In particular this holds when $Q = Q_{p,q}(a)$ for any $a \in \Sigma_{pq}$.

Proof. It is sufficient to prove this for words $w \in \Sigma_{pq}^2$ of length 2. Let $a \in Q$ be arbitrary and $b = f_{p/q,pq}(a, w[1], w[2])$. By Lemma 3.3.9 $f_{p/q,pq}(Qw) \subseteq Q_{p,q}(b)$. To prove equality it is sufficient to show that $\left|f_{p/q,pq}(Qw)\right| = q$, but this follows from Lemma 3.3.6. □

Consider two configurations that represent the same number in base 6, e.g. $\cdots 000.300 \cdots$ and $\cdots 000.255 \cdots$ that represent the number 1/2. From the facts that $\Pi_{3/2,6}$ is bijective and maps finite configurations to finite configurations it follows that these two configurations are mapped to $\cdots 000.4300 \cdots$ and $\cdots 000.4255 \cdots$ respectively, i.e. to the two base-6 representatives of the number 3/4. In this case one can also observe that the infinite sequences $300 \cdots$ and $255 \cdots$ are shifted by one position to the right by the action of $\Pi_{3/2,6}$. This observation is generalized in the following lemma and its corollary.

Lemma 3.3.11. Let $Q = \{np \mid 1 \leq n < q\} \subseteq \Sigma_{pq}$. For any $s \in Q$, $j \in \mathbb{Z}$ define $e_{s,j}, e_{s-1,j} \in \Sigma_{pq}^{\mathbb{Z}}$ by

$$e_{s,j}[i] = \begin{cases} s \text{ when } i = j, \\ 0 \text{ when } i > j, \end{cases} \qquad e_{s-1,j}[i] = \begin{cases} s-1 \text{ when } i = j, \\ pq-1 \text{ when } i > j \end{cases}$$

(their values at $i < j$ are irrelevant). For any $x \in \Sigma_{pq}^{\mathbb{Z}}$, $s \in Q$ and $j \in \mathbb{Z}$ there exist $x' \in \Sigma_{pq}^{\mathbb{Z}}$ and $s' \in Q$ such that

$$x_1 \doteqdot \Pi_{p,pq}(x \otimes_j e_{s,j}) = x' \otimes_j e_{s',j} \quad \text{and} \quad x_2 \doteqdot \Pi_{p,pq}(x \otimes_j e_{s-1,j}) = x' \otimes_j e_{s'-1,j}.$$

Proof. Clearly $x_1[i] = x_2[i]$ for $i \leq j-2$. The claim that $x_1[i] = 0$ and $x_2[i] = pq-1$ for $i > j$ follows by checking that $g_{p,pq}(0,0) = 0$ and $g_{p,pq}(pq-1, pq-1) = pq-1$. It remains to show that $x_1[j-1] = x_2[j-1]$, $x_1[j] = s'$ and $x_2[j] = s'-1$ for some $s' \in Q$.

Let us write $x[j-1] = a_1 q + a_0$, $s = s_1 q + s_0$ and $s-1 = s_1 q + (s_0 - 1)$ where $a_1, s_1 \in \Sigma_p$ and $a_0, s_0, s_0 - 1 \in \Sigma_q$: this is possible because s is not divisible by q. Then

$$\begin{aligned} x_1[j-1] &= g_{p,pq}(x[j-1], s) = a_0 p + s_1 = g_{p,pq}(x[j-1], s-1) = x_2[j-1], \\ x_1[j] &= g_{p,pq}(s, 0) = g_{p,pq}(s_1 q + s_0, 0q + 0) = s_0 p \doteqdot s' \in Q, \\ x_2[j] &= g_{p,pq}(s-1, pq-1) = g_{p,pq}(s_1 q + (s_0 - 1), (p-1)q + (q-1)) \\ &= (s_0 - 1)p + (p-1) = s' - 1. \end{aligned}$$

□

Corollary 3.3.12. Using the notation of the previous lemma, for any $x \in \Sigma_{pq}^{\mathbb{Z}}$, $s \in Q$ and $j \in \mathbb{Z}$ there exist $x' \in \Sigma_{pq}^{\mathbb{Z}}$ and $s' \in Q$ such that

$$\Pi_{p/q,pq}(x \otimes_j e_{s,j}) = x' \otimes_{j+1} e_{s',j+1} \quad \text{and} \quad \Pi_{p/q,pq}(x \otimes_j e_{s-1,j}) = x' \otimes_j e_{s'-1,j+1}.$$

3.4 The Trace Subshifts of Fractional Multiplication Automata

In this section we assume that $p > q > 1$ are coprime integers unless otherwise specified. We will show that the trace subshift $\Xi(\Pi_{p/q,pq})$ is not sofic.

To simplify the notation, we will denote for coprime $s, t > 1$ (not necessarily $s > t$) $\mathrm{Tr}_{s/t,I}(x) = \mathrm{Tr}_{\Pi_{s/t,st},I}(x)$, $\Xi_{s/t} = \Xi(\Pi_{s/t,st})$, $L(s/t) = L(\Xi_{s/t})$, $\mathrm{succ}_{s/t} = \mathrm{succ}_{\Xi_{s/t}}$ and $\mathrm{pred}_{s/t} = \mathrm{pred}_{\Xi_{s/t}}$. We will abuse notation and define the trace with respect to $\Pi_{s/t,st}$ also for positive real numbers.

Definition 3.4.1. For $\xi \in \mathbb{R}_{>0}$ we call sequence

$$\mathrm{Tr}_{s/t}(\xi) = \mathrm{Tr}_{s/t}(\mathrm{config}_{st}(\xi))$$

the *trace s/t-representation* of ξ.

Since $\mathrm{config}_{st}(\mathbb{R}_{>0})$ is a dense subset of $\Sigma_{st}^{\mathbb{Z}}$, it follows that $\Xi_{s/t}$ is the topological closure of $\mathrm{Tr}_{s/t}(\mathbb{R}_{>0})$.

Following [1], let $\psi_{p/q} : \mathbb{R}_{>0} \to \mathbb{Z}$ be the function defined by

$$\psi_{p/q}(\xi) = q\left\lfloor \frac{p}{q}\xi \right\rfloor - p\lfloor \xi \rfloor = p\,\mathrm{frac}(\xi) - q\,\mathrm{frac}\left(\frac{p}{q}\xi\right).$$

This function is periodic of period q and for every $\xi \in \mathbb{R}_{>0}$, $\psi_{p/q}(\xi)$ belongs to the set

$$\Sigma_{-q,p} \doteqdot \{-(q-1), \ldots, 0, 1, \ldots (p-1)\}.$$

Definition 3.4.2. For every $\xi \in \mathbb{R}_{>0}$, the infinite sequence $\varphi_{p/q}(\xi) \subseteq \Sigma_{-q,p}^{\mathbb{Z}}$ defined by

$$\varphi_{p/q}(\xi)[i] = \psi_{p/q}\left(\left(\frac{p}{q}\right)^i \xi\right) \text{ for every } i \in \mathbb{Z}$$

is called the *companion p/q-representation* of ξ. The topological closure of $\varphi_{p/q}(\mathbb{R}_{>0}) \subseteq \Sigma_{-q,p}^{\mathbb{Z}}$ is a subshift denoted by $Y_{p/q}$.

The subscript p/q is omitted from all notations when it is clear from the context.

The name "companion p/q-representation" was introduced in [1], probably to signify its connection to another type of a number representation system considered in the same paper. We adopt the same name because it will turn out that the companion p/q-representations are also strongly connected to trace p/q-representations. The earliest occurrence of the sequence $\varphi(\xi)$ seems to be in a paper of Forman and Shapiro [19] (where it has not been named). This representation, and its generalizations, also comes up in a sequence of papers by Dubickas starting from [16].

The following lemma shows that $\varphi(\xi)$ really is in some sense a representation of ξ in base p/q.

Lemma 3.4.3. $\operatorname{frac}(\xi) = \frac{1}{p}\sum_{i=0}^{\infty}\left(\frac{q}{p}\right)^i \varphi(\xi)[i]$ for every $\xi \in \mathbb{R}_{>0}$.

Proof. For $i \in \mathbb{N}$ denote $y_i = \operatorname{frac}((p/q)^i\xi)$ and $s_i = \varphi(\xi)[i] = py_i - qy_{i+1}$. From this we can solve

$$y_0 = \frac{1}{p}s_0 + \frac{q}{p}y_1 = \frac{1}{p}s_0 + \frac{1}{p}\frac{q}{p}s_1 + \left(\frac{q}{p}\right)^2 y_2 = \cdots = \frac{1}{p}\sum_{i=0}^{\infty}\left(\frac{q}{p}\right)^i s_i.$$

□

Definition 3.4.4. For $n > 1$ define $\mathrm{Md}_n : \mathbb{Z} \to \Sigma_n$ by

$$\mathrm{Md}_n(m) = m - n\lfloor m/n \rfloor,$$

i.e. $\mathrm{Md}_n(m)$ is the remainder of m divided by n. It can be extended to a function $\mathbb{Z}^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ by coordinatewise application.

Definition 3.4.5. For every $x \in \Sigma_{pq}^{\mathbb{Z}}$ define the bi-infinite sequence $\Phi(x)$ by

$$\Phi(x)[i] = q\,\mathrm{Md}_p(x[i+1]) - p\,\mathrm{Md}_q(x[i]) \text{ for every } i \in \mathbb{Z}.$$

The map Φ connects the two different p/q representations.

Theorem 3.4.6. $\Phi(\mathrm{Tr}(\xi)) = \varphi(\xi)$ for every $\xi \in \mathbb{R}_{>0}$.

Proof. For every $i \in \mathbb{Z}$ we can write

$$\left(\frac{p}{q}\right)^i \xi = n_i q + a_i + \xi_i,$$

where $n_i \in \mathbb{N}$, $a_i \in \Sigma_q$ and $\xi_i \in [0,1)$ are unique. Then

$$\left(\frac{p}{q}\right)^{i+1} \xi = n_i p + \frac{p}{q}(a_i + \xi_i) = n_i p + b_i + \xi_i'$$

for unique $b_i \in \Sigma_p$ and $\xi_i' \in [0,1)$, because $\frac{p}{q}(a_i + \xi_i) \in [0,p)$. Thus

$$\begin{aligned}
\varphi(\xi)[i] = \psi_{p/q}\left(\left(\frac{p}{q}\right)^i \xi\right) &= q \left\lfloor \left(\frac{p}{q}\right)^{i+1} \xi \right\rfloor - p \left\lfloor \left(\frac{p}{q}\right)^i \xi \right\rfloor \\
&= q\lfloor n_i p + b_i + \xi_i' \rfloor - p\lfloor n_i q + a_i + \xi_i \rfloor = q b_i - p a_i \\
&= q \operatorname{Md}_p(\operatorname{Tr}(\xi)[i+1]) - p \operatorname{Md}_q(\operatorname{Tr}(\xi)[i]) = \Phi(\operatorname{Tr}(\xi))[i].
\end{aligned}$$

□

The correspondence between the two p/q representations extends to the level of the induced subshifts $\Xi_{p/q}$ and $Y_{p/q}$.

Theorem 3.4.7. $\Phi : \Xi_{p/q} \to Y_{p/q}$ is a conjugacy.

Proof. We first prove that Φ is injective on $\Sigma_{pq}^{\mathbb{Z}}$. To see this, assume that $x, y \in \Sigma_{pq}^{\mathbb{Z}}$ are elements such that $\Phi(x) = \Phi(y)$ and let $i \in \mathbb{Z}$. Then

$$\begin{aligned}
&\Phi(x)[i-1] = \Phi(y)[i-1] \\
\Longrightarrow\ & q \operatorname{Md}_p(x[i]) - p \operatorname{Md}_q(x[i-1]) = q \operatorname{Md}_p(y[i]) - p \operatorname{Md}_q(y[i-1]) \\
\Longrightarrow\ & q \operatorname{Md}_p(x[i]) \equiv q \operatorname{Md}_p(y[i]) \pmod p \implies x[i] \equiv y[i] \pmod p
\end{aligned}$$

and

$$\begin{aligned}
&\Phi(x)[i] = \Phi(y)[i] \\
\Longrightarrow\ & q \operatorname{Md}_p(x[i+1]) - p \operatorname{Md}_q(x[i]) = q \operatorname{Md}_p(y[i+1]) - p \operatorname{Md}_q(y[i]) \\
\Longrightarrow\ & p \operatorname{Md}_q(x[i]) \equiv p \operatorname{Md}_q(y[i]) \pmod q \implies x[i] \equiv y[i] \pmod q.
\end{aligned}$$

Because $x[i], y[i] \in \Sigma_{pq}$, it follows that $x[i] = y[i]$ for all $i \in \mathbb{Z}$.

Since $\Phi : \Sigma_{pq}^{\mathbb{Z}} \to \Phi(\Sigma_{pq}^{\mathbb{Z}})$ is a continuous injective map on a compact metrizable space, it is a homeomorphism. Using the previous theorem we can deduce that

$$\Phi(\Xi_{p/q}) = \Phi(\overline{\operatorname{Tr}_{p/q}(\mathbb{R}_{>0})}) = \overline{\Phi(\operatorname{Tr}_{p/q}(\mathbb{R}_{>0}))} = \overline{\varphi(\mathbb{R}_{>0})} = Y_{p/q} :$$

because Φ is a homeomorphism, we can change the order of taking a topological closure and applying Φ. Therefore the restriction map $\Phi : \Xi_{p/q} \to Y_{p/q}$ is continuous and bijective.

Consider now Φ restricted to $\Xi_{p/q}$. We need to show that $\Phi \circ \sigma = \sigma \circ \Phi$. Since these are continuous maps, it is sufficient to prove that they agree on the dense set $\mathrm{Tr}_{p/q}(\mathbb{R}_{>0}) \subseteq \Xi_{p/q}$. For $\xi \in \mathbb{R}_{>0}$ and $x = \mathrm{config}_{pq}(\xi)$ we verify that

$$\begin{aligned}
&\Phi(\sigma(\mathrm{Tr}_{p/q}(\xi))) = \Phi(\sigma(\mathrm{Tr}_{p/q}(x))) = \Phi(\mathrm{Tr}_{p/q}(\Pi_{p/q,pq}(x))) \\
&= \Phi(\mathrm{Tr}_{p/q}((p/q)\xi)) \overset{T3.4.6}{=} \varphi((p/q)\xi) = \sigma(\varphi(\xi)) \overset{T3.4.6}{=} \sigma(\Phi(\mathrm{Tr}_{p/q}(\xi))).
\end{aligned}$$

□

A special case of Lemma 1 in [16] says that $\varphi_{p/q}(\xi)$ is not eventually periodic for $\xi \in \mathbb{R}_{>0}$. The last two theorems together with Proposition 3.3.5 yield an alternative proof of this fact.

We begin to examine the properties of the language $L(p/q)$ with the aim of proving that $\Xi_{p/q}$ is not sofic.

Lemma 3.4.8. If $a_1, a_2, b_1, b_2 \in \Sigma_{pq}$, $w \in \Sigma_{pq}^n$ for some n, $a_1 \not\equiv a_2 \pmod q$ and $b_1 \not\equiv b_2 \pmod p$, then $\{a_i w b_j \mid i,j \in \{1,2\}\} \not\subseteq L(p/q)$.

Proof. Assume to the contrary that $\{a_i w b_j \mid i,j \in \{1,2\}\} \subseteq L(p/q)$. Without loss of generality $m_q = \mathrm{Md}_q(a_2) - \mathrm{Md}_q(a_1) > 0$ and $m_p = \mathrm{Md}_p(b_1) - \mathrm{Md}_p(b_2) > 0$. Let $\xi_1, \xi_2 \in \mathbb{R}_{>0}$ be such that $\mathrm{Tr}(\xi_i)[0, n+1] = a_i w b_i$ for $i \in \{1,2\}$. For any $\xi \in \mathbb{R}_{>0}$ we have

$$\begin{aligned}
&\frac{1}{q^{n+1}} \psi_{p^{n+1}/q^{n+1}}(\xi) = \left\lfloor \left(\frac{p}{q}\right)^{n+1} \xi \right\rfloor - \left(\frac{p}{q}\right)^{n+1} \lfloor \xi \rfloor \\
&= \sum_{i=0}^{n} \left(\frac{p}{q}\right)^i \left(\left\lfloor \left(\frac{p}{q}\right)^{n-i+1} \xi \right\rfloor - \left(\frac{p}{q}\right) \left\lfloor \left(\frac{p}{q}\right)^{n-i} \xi \right\rfloor \right) \\
&= \frac{1}{q} \sum_{i=0}^{n} \left(\frac{p}{q}\right)^i \varphi_{p/q}(\xi)[n-i] \\
&\overset{T3.4.6}{=} \frac{1}{q} \sum_{i=0}^{n} \left(\frac{p}{q}\right)^i (q\,\mathrm{Md}_p(\mathrm{Tr}(\xi)[n-i+1]) - p\,\mathrm{Md}_q(\mathrm{Tr}(\xi)[n-i])),
\end{aligned}$$

and because $\mathrm{Tr}(\xi_1)[1,n] = \mathrm{Tr}(\xi_2)[1,n]$, it follows that

$$\begin{aligned}
&\psi_{p^{n+1}/q^{n+1}}(\xi_1) - \psi_{p^{n+1}/q^{n+1}}(\xi_2) \\
&= q^n \left(q\,\mathrm{Md}_p(\mathrm{Tr}(\xi_1)[n+1]) - \left(\frac{p}{q}\right)^n p\,\mathrm{Md}_q(\mathrm{Tr}(\xi_1)[0]) \right) \\
&- q^n \left(q\,\mathrm{Md}_p(\mathrm{Tr}(\xi_2)[n+1]) - \left(\frac{p}{q}\right)^n p\,\mathrm{Md}_q(\mathrm{Tr}(\xi_2)[0]) \right) \\
&= q^n \left(q m_p + \left(\frac{p}{q}\right)^n p m_q \right) = q^{n+1} m_p + p^{n+1} m_q \geq q^{n+1} + p^{n+1}
\end{aligned}$$

which contradicts the fact that $\psi_{p^{n+1}/q^{n+1}}(\xi) \in \Sigma_{-q^{n+1},p^{n+1}}$ for all $\xi \in \mathbb{R}_{>0}$. $\square$

Lemma 3.4.9. Let $s, t > 1$ be coprime (we do not assume that $s > t$). If $wa \in L(s/t)$ for some $w \in \Sigma_{st}^{+}$ and $a \in \Sigma_{st}$, then $wQ_{s,t}(a) \subseteq L(s/t)$.

Proof. Let $x \in \Sigma_{st}^{\mathbb{Z}}$ such that $\mathrm{Tr}_{s/t}(x)[0, |wa|-1] = wa$ and for every $d \in \Sigma_{st}$ let $x_d \in \Sigma_{st}^{\mathbb{Z}}$ be such that $x_d(-|w|) = d$ and $x_d[i] = x[i]$ for $i \neq -|w|$. Then

$$\{\mathrm{Tr}_{s/t}(x_d)[0, |wa|-1] \mid d \in \Sigma_{st}^{\mathbb{Z}}\} = wQ_{s,t}(a)$$

by repeated application of Proposition 3.3.10. $\square$

Lemma 3.4.10. For any $a \in \Sigma_{pq}$ it holds that

$$\left| f_{q/p,pq}(0, a, \Sigma_{pq}) \right| = \begin{cases} 2 \text{ when } \mathrm{Md}_p(aq) \in \{p - i \mid 1 \leq i \leq q-1\}, \\ 1 \text{ otherwise.} \end{cases}$$

Moreover, in the first case, there are $d_a, b_{a,1}, b_{a,2} = b_{a,1} + 1 \in \Sigma_{pq}$ such that $b_{a,2}$ is divisible by p and $f_{q/p,pq}(0, a, b_{a,1}) = d_a$, $f_{q/p,pq}(0, a, b_{a,2}) = d_a + 1$.

Proof. For $a, b \in \Sigma_{pq}$ write $a = a_1 p + a_0$ and $b = b_1 p + b_0$. Then

$$f_{q/p,pq}(0, a, b) = g_{q,pq}(g_{q,pq}(0, a), g_{q,pq}(a, b)) = g_{q,pq}(a_1, a_0 q + b_1) = \mathrm{Md}_p(a_1)q + d,$$

where $d = \left\lfloor \frac{a_0 q + b_1}{p} \right\rfloor$. If b ranges over Σ_{pq}, then b_1 ranges over Σ_q and d can attain two distinct values if and only if $\mathrm{Md}_p(aq) = \mathrm{Md}_p(a_0 q) \in \{p - i \mid 1 \leq i \leq q-1\}$.

If d can attain two distinct values, then there is a unique $c \in \Sigma_q \setminus \{q-1\}$ such that $\left\lfloor \frac{a_0 q + c}{p} \right\rfloor < \left\lfloor \frac{a_0 q + (c+1)}{p} \right\rfloor$. Then we can choose $b_{a,1} = cp + (p-1)$ and $b_{a,2} = (c+1)p$. $\square$

Lemma 3.4.11. For any $a \in \Sigma_{pq}$ there is a $d \in \Sigma_{pq}$ such that

$$\mathrm{pred}_{p/q}(a) = \begin{cases} Q_{q,p}(d) \cup Q_{q,p}(d+1) \text{ if } \mathrm{Md}_p(aq) \in \{p - i \mid 1 \leq i \leq q-1\}, \\ Q_{q,p}(d) \text{ otherwise.} \end{cases}$$

In particular, $\left| \mathrm{pred}_{p/q}(a) \right|$ is equal to $2p$ or p respectively.

Proof. If $\mathrm{Md}_p(aq) \in \{p - i \mid 1 \leq i \leq q-1\}$, then by the previous lemma there is a partition $B_1 \cup B_2 = \Sigma_{pq}$ such that $f_{q/p,pq}(0, a, B_1) = d$ and $f_{q/p,pq}(0, a, B_2) = d+1$ for some $d \in \Sigma_{pq}$. Then from Proposition 3.3.10 it follows that $f_{q/p,pq}(\Sigma_{pq}, a, B_1) = Q_{q,p}(d)$ and $f_{q/p,pq}(\Sigma_{pq}, a, B_2) = Q_{q,p}(d+1)$, so $\mathrm{pred}_{p/q}(a) = Q_{q,p}(d) \cup Q_{q,p}(d+1)$. This is a set of cardinality $2p$. The proof for $\mathrm{Md}_p(aq) \notin \{p - i \mid 1 \leq i \leq q-1\}$ is similar. $\square$

Lemma 3.4.12. For any $w \in L(p/q)\setminus\{\epsilon\}$ there is a $d \in \Sigma_{pq}$ such that either $\mathrm{pred}_{p/q}(w) = Q_{q,p}(d) \cup Q_{q,p}(d+1)$ or $\mathrm{pred}_{p/q}(w) = Q_{q,p}(d)$. In particular, $\left|\mathrm{pred}_{p/q}(w)\right|$ is equal to $2p$ or p.

Proof. Consider an arbitrary word $w = av \in L(p/q)$, where $v \in \Sigma_{pq}^*$ and $a \in \Sigma_{pq}$. Evidently $\mathrm{pred}_{p/q}(av) \neq \emptyset$ and by the previous lemma $\mathrm{pred}_{p/q}(av) \subseteq \mathrm{pred}_{p/q}(a) \subseteq Q_{q,p}(d) \cup Q_{q,p}(d+1)$ for some $d \in \Sigma_{pq}$. Then from Lemma 3.4.9 it follows that $\mathrm{pred}_{p/q}(av) = \bigcup_{i\in\mathcal{I}} Q_{q,p}(d+i)$ for some nonempty set $\mathcal{I} \subseteq \{0,1\}$. $\square$

Based on this lemma we define two sets of words for every $n \in \mathbb{N}_+$:

$$W_{1,n} = \{w \in L(p/q) \cap \Sigma_{pq}^n \mid \left|\mathrm{pred}_{p/q}(w)\right| = p\}$$
$$W_{2,n} = \{w \in L(p/q) \cap \Sigma_{pq}^n \mid \left|\mathrm{pred}_{p/q}(w)\right| = 2p\}.$$

These form a partition $L(p/q) \cap \Sigma_{pq}^n = W_{1,n} \cup W_{2,n}$. In the next two lemmas we show how to find all elements of $W_{2,n}$ in the traces of suitable configurations.

Lemma 3.4.13. Let $s \in Q$ and $e_{s,0}$ be as in Lemma 3.3.11. Then we have $\mathrm{Tr}_{p/q}(x \otimes_0 e_{s,0})[1,n] \in W_{2,n}$ for every $x \in \Sigma_{pq}^{\mathbb{Z}}$ and $n \in \mathbb{N}_+$.

Proof. Let $w = \mathrm{Tr}_{p/q}(x \otimes_0 e_{s,0})[1,n]$. By Corollary 3.3.12

$$\mathrm{Tr}_{p/q}(x \otimes_0 e_{s,0})[1,n] = \mathrm{Tr}_{p/q}(x \otimes_0 e_{s-1,0})[1,n],$$

so we have $sw, (s-1)w \in L(p/q)$. By Lemma 3.4.9 $\mathrm{pred}_{p/q}(w)$ contains at least $2p$ words, so $w \in W_{2,n}$. $\square$

Lemma 3.4.14. Let $Q = \{np \mid 1 \leq n < q\}$ and fix $n \in \mathbb{N}_+$. For every $s \in Q$ the set

$$W_s = \{\mathrm{Tr}_{p/q}(x)[1,n] \mid x \in \Sigma_{pq}^{\mathbb{Z}}, x[0] = s, x[i] = 0 \text{ for } i > 0\} \subseteq W_{2,n}$$

contains q^n elements, $W_{2,n} = \bigcup_{s\in Q} W_s$ and $|W_{2,n}| = q^n(q-1)$.

Proof. Denote $W = \bigcup_{s\in Q} W_s$. We begin by showing that $W \subseteq W_{2,n}$ and that $|W| = q^n(q-1)$. First, $W_s \subseteq W_{2,n}$ follows from the previous lemma, and by repeated application of Proposition 3.3.10 it follows that $|W_s| = q^n$. To prove that $|W| = q^n(q-1)$ it is enough to show that $W_s \cap W_{s'} = \emptyset$ for distinct $s, s' \in Q$. This in turn follows by showing that $f_{p/q,pq}(a, s, 0) \neq f_{p/q,pq}(b, s', 0)$ for all $a, b \in \Sigma_{pq}$. Therefore let $a = a_1 q + a_0$, $b = b_1 q + b_0$, $s = s_1 q + s_0$ and $s' = s'_1 q + s'_0$. Let $d_1, d'_1 \in \Sigma_p$ and $d_0, d'_0 \in \Sigma_q$ be such that $s_0 p = d_1 q + d_0$ and $s'_0 p = d'_1 q + d'_0$. Since $s, s' \in Q$, we have $s \not\equiv s' \pmod q$

so the values $s_0, s_0' \in \Sigma_q$ are distinct. Then $|s_0 p - s_0' p| \geq p > q$, so $d_1 \neq d_1'$. We compute

$$\begin{aligned}
&f_{p/q,pq}(a, s, 0) = g_{p,pq}(g_{p,pq}(a, s), g_{p,pq}(s, 0)) = g_{p,pq}(a_0 p + s_1, s_0 p) \\
&= \mathrm{Md}_q(a_0 p + s_1)p + d_1 \not\equiv \mathrm{Md}_q(b_0 p + s_1')p + d_1' = f_{p/q,pq}(b, s', 0) \pmod{p}.
\end{aligned}$$

To prove the inclusion $W_{2,n} \subseteq W$ it is now sufficient to show that $|W_{2,n}| = q^n(q-1)$. The proof is by induction. The case $n = 1$ follows from Lemma 3.4.11, so let us assume that the claim holds for some $n \in \mathbb{N}_+$. By the previous paragraph $|W_{2,n+1}| \geq q^{n+1}(q-1)$, so let us assume contrary to our claim that $|W_{2,n+1}| > q^{n+1}(q-1)$. Every element of $W_{2,n+1}$ is of the form wa where $w \in W_{2,n}$ and $a \in \Sigma_{pq}$, so by pigeonhole principle there exist $w \in W_{2,n}$ and letters $a_1, a_2, \ldots, a_k \in \Sigma_{pq}$ with $k > q$ such that $wa_i \in W_{2,n+1}$ for all $1 \leq i \leq k$. Without loss of generality $a_1 \not\equiv a_2 \pmod{p}$ and $\mathrm{pred}_{p/q}(wa_1) = \mathrm{pred}_{p/q}(w) = \mathrm{pred}_{p/q}(wa_2)$, which contradicts Lemma 3.4.8. □

This characterization of the set $W_{2,n}$ will be of use in proving that $\Xi_{p/q}$ is not sofic. As a byproduct we found the cardinality of $W_{2,n}$, which allows us to compute the complexity function of $\Xi_{p/q}$.

Theorem 3.4.15. $P_{\Xi_{p/q}}(n) = pq(p^{n-1} - q^{n-1})\frac{q-1}{p-q} + p^n q$ for every $n \in \mathbb{N}_+$.

Proof. The proof is by induction. In the case $n = 1$ the expression equals pq, so let us assume that the equation holds for some $n \in \mathbb{N}_+$. Then

$$\begin{aligned}
&P_{\Xi_{p/q}}(n+1) = 2p|W_{2,n}| + p|W_{1,n}| = 2p|W_{2,n}| + p(P_{\Xi_{p/q}}(n) - |W_{2,n}|) \\
&= p(|W_{2,n}| + P_{\Xi_{p/q}}(n)) = p\left(q^n(q-1) + pq(p^{n-1} - q^{n-1})\frac{q-1}{p-q} + p^n q\right) \\
&= pq^n(q-1)\frac{p-q}{p-q} + p^2 q(p^{n-1} - q^{n-1})\frac{q-1}{p-q} + p^{n+1} q \\
&= \left(pq^n(p-q) + p^2 q(p^{n-1} - q^{n-1})\right)\frac{q-1}{p-q} + p^{n+1} q \\
&= \left(p^2 q^n - pq^{n+1} + p^{n+1} q - p^2 q^n\right)\frac{q-1}{p-q} + p^{n+1} q \\
&= pq(p^n - q^n)\frac{q-1}{p-q} + p^{n+1} q.
\end{aligned}$$

□

Example 3.4.16. For $p/q = 3/2$, this is $6(3^{n-1} - 2^{n-1}) + 3^n \cdot 2 = 4 \cdot 3^n - 3 \cdot 2^n$. The first few terms are $6, 24, 84, 276, 876, \ldots$

Lemma 3.4.17. Let $Q = \{np \mid 1 \leq n < q\}$, $j \in \mathbb{Z}$ and $x \in \Sigma_{pq}^{\mathbb{Z}}$ such that $x[j] \in Q$ and $x[i] = 0$ for $i > j$. Then $\mathrm{Tr}_{p/q}(x)$ is not eventually periodic.

Proof. Assume to the contrary that there are $N \in \mathbb{N}$, $P \in \mathbb{N}_+$ such that $\mathrm{Tr}_{p/q}(x)[i] = \mathrm{Tr}_{p/q}(x)[i+P]$ for $i \geq N$. By Lemma 3.3.12 we can see that $\Pi^N_{p/q,pq}(x)[j+N] \in Q$ and $\Pi^N_{p/q,pq}(x)[i+N] = 0$ for $i > j$, so without loss of generality (by considering the configuration $\Pi^M_{p/q,pq}(x)$ instead of x for sufficiently large M if necessary) $N = 0$ and $j \geq 0$.

For each $n \in \mathbb{N}_+$ let $x_n = 0^{\mathbb{Z}} \otimes_{-((n+1)P+1)} x$, so for every $0 \leq i \leq nP+1$ it holds that

$$\mathrm{Tr}_{p/q}(x_n)[i] = \mathrm{Tr}_{p/q}(x)[i] = \mathrm{Tr}_{p/q}(x)[i+P] = \mathrm{Tr}_{p/q}(x_n)[i+P].$$

By Theorem 3.4.6 $\Phi(\mathrm{Tr}(x_n)) = \varphi(\mathrm{real}(x_n))$, so it follows that

$$\varphi(\mathrm{real}(x_n))[i] = \varphi(\mathrm{real}(x_n))[i+P] = \varphi\left(\left(\frac{p}{q}\right)^P \mathrm{real}(x_n)\right)[i] \text{ for } 0 \leq i \leq nP,$$

which by Lemma 3.4.3 implies that $\left|\mathrm{frac}(\mathrm{real}(x_n)) - \mathrm{frac}((p/q)^P \mathrm{real}(x_n))\right| = \mathcal{O}((q/p)^{nP})$. On the other hand, by Lemma 3.3.12

$$x_n[j] \in Q, \quad \Pi^P_{p/q,pq}(x_n)[j+P] \in Q, \quad x_n[i] = \Pi^P_{p/q,pq}(x_n)[i+P] = 0 \text{ for } i > j.$$

Since x_n and $\Pi^P_{p/q,pq}(x_n)$ are base-pq representations of the numbers $\mathrm{real}(x_n)$ and $(p/q)^P \mathrm{real}(x_n)$, it follows that

$$\left|\mathrm{frac}(\mathrm{real}(x_n)) - \mathrm{frac}((p/q)^P \mathrm{real}(x_n))\right| \geq (pq)^{-(j+P)},$$

a contradiction for sufficiently big $n \in \mathbb{N}_+$. □

Theorem 3.4.18. The subshift $\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}$ is not sofic.

Proof. Assume to the contrary that $\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}$ is sofic. We define $z \in \Sigma_{pq}^{\mathbb{Z}}$ as follows. First let $z[0] = p$ and $z[i] = 0$ for $i \in \mathbb{N}_+$. Now let $i \in \mathbb{N}_+$ and assume that $z[0], \dots, z[-(i-1)]$ have been defined. By the permutivity property of Proposition 3.3.10 we can define $z[-i]$ in such a way that $\mathrm{Tr}_{p/q}(z)[i] \in \Sigma_p$. By Lemma 3.4.14 the inclusion $\mathrm{Tr}_{p/q}(z)[1,n] \in W_{2,n}$ holds for all $n \in \mathbb{N}_+$. A compactness argument together with Lemma 3.4.12 shows that $\mathrm{pred}_{p/q}(\mathrm{Tr}_{p/q}(z)[1,\infty]) = Q_{q,p}(d) \cup Q_{q,p}(d+1)$ for some $d \in \Sigma_{pq}$. We can choose $a \in Q_{q,p}(d) \cap \Sigma_p$ and $b \in Q_{q,p}(d+1) \cap \Sigma_p$ so in particular $a \not\equiv b \pmod{q}$.

We define $x_1, x_2 \in \Xi_{p/q}$ as follows. First let $x_1[0,\infty] = a\,\mathrm{Tr}_{p/q}(z)[1,\infty]$ and $x_2[0,\infty] = b\,\mathrm{Tr}_{p/q}(z)[1,\infty]$. Now let $i \in \mathbb{N}_+$ and assume inductively that $x_1[0], \dots, x_1[-(i-1)]$ have been defined so that all prefixes of $x[-(i-1),\infty]$ are in $L(\Xi_{p/q}) \cap \Sigma_p^*$. By Lemma 3.4.9 and by compactness there exists $e \in \Sigma_{pq}$ such that $Q_{q,p}(e) \subseteq \mathrm{pred}_{p/q}(x[-(i-1),\infty])$. Then choose arbitrarily $x[i] \in Q_{q,p}(e) \cap \Sigma_p$. All the subwords of x_1 belong to $L(\Xi_{p/q}) \cap \Sigma_p^*$ and therefore $x_1 \in \Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}$. By the same argument we define x_2 so that $x_2 \in \Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}$.

Define $x \in (\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}) \times (\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}) \subseteq (\Sigma_p^2)^{\mathbb{Z}}$ by $x[i] = (x_1[i], x_2[i])$ for $i \in \mathbb{Z}$. Since $(\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}) \times (\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}})$ is also sofic, by the pumping lemma of regular languages there exist $N, P \in \mathbb{N}_+$ such that

$$y_i = x_i[-\infty, N-1]x_i[N, N+P-1]^\infty \in \Xi_{p/q} \text{ for } i \in \{1,2\}.$$

Because $y_1[0] = x_1[0] = a \not\equiv b = x_2[0] = y_2[0] \pmod q$ and $y_1[i] = y_2[i]$ for $i > 0$, it follows that $y_1[1,n] \in W_{2,p}$ for every $n \in \mathbb{N}_+$, so by compactness and by Lemma 3.4.14 there exists $y \in \Sigma_{pq}^{\mathbb{Z}}$ such that $y[0] \in Q = \{np \mid 1 \leq n < q\}$, $y[i] = 0$ for $i > 0$ and $\mathrm{Tr}_{p/q}(y)[1,\infty] = y_1[1,\infty]$: in particular $\mathrm{Tr}_{p/q}(y)[i] = \mathrm{Tr}_{p/q}(x)[i+P]$ for every $i \geq N$, which contradicts the previous lemma. □

Corollary 3.4.19. The subshift $\Xi_{p/q}$ is not sofic. In particular, the CA $\Pi_{p/q,pq}$ is not regular.

Proof. Assume to the contrary that $\Xi_{p/q}$ is sofic. Then $\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}$ is also sofic as the intersection of two sofic subshifts, but this is impossible by the previous theorem. □

We mention in passing that Jalonen and Kari show in Proposition 6 of [27] that there exists a reversible CA on a full shift which is left expansive (stated in [27] for right expansive CA) and has a non-sofic trace subshift. The previous corollary gives an alternative proof of this fact, because it follows from Proposition 3.3.4 that $\Pi_{p/q,pq}$ is left expansive.

3.5 Trace Subshifts and the Distribution of Fractional Parts $\mathrm{frac}(\xi(p/q)^i))$

In this section we assume that $p > q > 1$ are coprime integers. Our study of the trace subshift $\Xi_{p/q}$ allows us to make progress on a generalized version of Mahler's problem. For any $S \subseteq \mathbb{R}$ we denote

$$Z_{p/q}(S) = \left\{ \xi > 0 \;\middle|\; \mathrm{frac}\left(\xi \left(\frac{p}{q}\right)^i\right) \in \mathrm{frac}(S) \text{ for every } i \in \mathbb{N} \right\}.$$

Note that in this definition only the fractional parts of S are considered, which allows us to write e.g. $Z_{p/q}([0,1/2) \cup [3/4,1)) = Z_{p/q}([3/4,3/2))$.

Mahler's question [45] is whether the set $Z_{3/2}([0,1/2))$ is empty or not. More generally, for all p,q it is an open problem whether $Z_{p/q}([0,1/q))$ is empty or not: the general consensus is that $Z_{p/q}([0,1/q))$ is empty. It is a result of Flatto, Lagarias and Pollington [18] that $Z_{p/q}(S) = \emptyset$ whenever $S \subseteq \mathbb{R}$ is an interval strictly shorter than $1/p$.

If $\xi \in \mathbb{R}_{>0}$ and $x = \mathrm{config}_{pq}(\xi)$, then $\xi \in [0,1/q)$ is equivalent to $x[1] \in \Sigma_p$. Therefore determining whether $Z_{p/q}([0,1/q))$ is nonempty is equivalent to determining whether there exists $\xi \in \mathbb{R}_{>0}$ such that $\mathrm{Tr}_{p/q,1}(x)[0,\infty] \in \Sigma_p^{\mathbb{Z}}$ for $x = \mathrm{config}_{pq}(\xi)$. The difficulty of making this determination may be connected to the fact that $\Xi_{p/q} \cap \Sigma_p^{\mathbb{Z}}$ is not a sofic subshift (Theorem 3.4.18). On the other hand, in the following it turns out that in the case $p \geq 2q-1$ there is a special digit set $D_{p,q} \subseteq \Sigma_{pq}$ such that $\Xi_{p/q} \cap D_{p,q}^{\mathbb{Z}}$ is an SFT (Corollary 3.5.6) and which can be used to find small finite unions of intervals $I_{p,q,k}$ such that $Z_{p/q}(I_{p,q,k}) \neq \emptyset$ (Theorem 3.5.12).

Definition 3.5.1. Let $p \geq 2q-1$. For every $d \in \Sigma_q$ let $k_d \in \Sigma_p$ be the unique digit such that $\mathrm{Md}_p(k_d q) = d$. Then let

$$D_{p,q} = \{a \in \Sigma_{pq} \mid a \equiv k_d \pmod{p} \text{ for some } d \in \Sigma_q\}.$$

To each k_d we associate $j_d \in \Sigma_q$ which is the unique element such that $k_d q = j_d p + d$.

Example 3.5.2. Consider the case $p = 3$ and $q = 2$. Then $\Sigma_q = \{0,1\}$ and $D_{3,2} = \{0,2,3,5\}$ consists of the elements of Σ_6 which are congruent to either $k_0 = 0$ or $k_1 = 2 \pmod 3$. We see that $2k_0 = 0 = 0 \cdot 3 + 0$ and $2k_1 = 4 = 1 \cdot 3 + 1$, so $j_0 = 0$ and $j_1 = 1$.

It turns out that $\Xi_{p/q} \cap D_{p,q}^{\mathbb{Z}}$ is an SFT for which we can give a simple characterization.

Lemma 3.5.3. The sets $Q_{q,p}(j_d) \cap D_{p,q}$ $(d \in \Sigma_q)$ form a partition of $D_{p,q}$ such that $|Q_{q,p}(j_d) \cap D_{p,q}| = q$.

Proof. The set $D_{p,q}$ is the union of q residue classes modulo p (within Σ_{pq}), so as a complete residue system modulo p the set $Q_{q,p}(j_d)$ intersects each of these classes by a single element and $|Q_{q,p}(j_d) \cap D_{p,q}| = q$. By definition all the numbers j_d are in different residue classes modulo q, so the sets $Q_{q,p}(j_d)$ are disjoint and $\left|\bigcup_{d \in \Sigma_q} Q_{q,p}(j_d) \cap D_{p,q}\right| = q^2$. This equals the cardinality of $D_{p,q}$, so the sets $Q_{q,p}(j_d) \cap D_{p,q}$ form a partition. □

Lemma 3.5.4. Let $p > q \geq 2$ be coprime such that $p \geq 2q-1$. For every $d \in \Sigma_q$ let $j_d \in \Sigma_q$ be the unique element such that $k_d q = j_d p + d$. If $aw \in L(p/q)$ for some $w \in \Sigma_{pq}^*$ and $a \in D_{p,q}$ such that $a \equiv k_d \pmod{p}$, then $\mathrm{pred}_{p/q}(aw) = Q_{q,p}(j_d)$.

Proof. To show the inclusion from left to right, assume that $b \in \operatorname{pred}_{p/q}(aw)$, so $b = f_{q/p,pq}(x,a,y)$ for some $x, y \in \Sigma_{pq}$. Let us write $a = a_1 p + a_0$, $y = y_1 p + y_0$, $g_{q,pq}(x,a) = z = z_1 p + z_0$ and $g_{q,pq}(a,y) = u = u_1 p + u_0$, where $a_0, y_0, z_0, u_0 \in \Sigma_p$ and $a_1, y_1, z_1, u_1 \in \Sigma_q$. Here $a_0 = k_d$ because $a \equiv k_d \pmod p$ and $u_1 = j_d$ because $g_{q,pq}(a,y) = k_d q + y_1 = j_d p + (d + y_1)$ and $d + y_1 \leq (q-1) + (q-1) < p$. Now

$$f_{q/p,pq}(x,a,y) = g_{q,pq}(g_{q,pq}(x,a), g_{q,pq}(a,y)) = g_{q,pq}(z,u) = z_0 q + j_d,$$

and thus $b \in Q_{q,p}(j_d)$.

Now we show the inclusion from right to left. Fix some $b \in \operatorname{pred}_{p/q}(aw)$, i.e. $baw \in L(p/q)$. By the previous paragraph $b \in Q_{q,p}(j_d)$ and therefore $Q_{q,p}(b) = Q_{q,p}(j_d)$. Now

$$Q_{q,p}(j_d)aw = Q_{q,p}(b)aw \overset{L3.4.9}{\subseteq} L(p/q),$$

which means that $Q_{q,p}(j_d) \subseteq \operatorname{pred}_{p/q}(aw)$. □

Lemma 3.5.5. Let $p \geq 2q-1$. For any $w \in L(p/q) \cap D_{p,q}^{+}$ there is a configuration $x \in \Xi_{p/q} \cap D_{p,q}^{\mathbb{Z}}$ in which w occurs.

Proof. It is sufficient to show that $\operatorname{pred}_{p/q}(w) \cap D_{p,q} \neq \emptyset$ and $\operatorname{succ}_{p/q}(w) \cap D_{p,q} \neq \emptyset$, because then the claim follows by induction and by compactness. By the previous lemma $\operatorname{pred}_{p/q}(w) \cap D_{p,q} = Q_{q,p}(j_d) \cap D_{p,q}$ for some $d \in \Sigma_q$ and by Lemma 3.5.3 this set is not empty.

Write now $w = w[1] \cdots w[k]$ for some $w[i] \in D_{p,q}$. By Lemma 3.5.3 there is some $d \in \Sigma_q$ such that $w[k] \in Q_{q,p}(j_d) \cap D_{p,q}$, so by the previous lemma $w[k] \in \operatorname{pred}_{p/q}(k_d)$. An induction using the previous lemma shows that $w[i] \cdots w[k] k_d \in L(p/q)$ for all $1 \leq i \leq k$ so in particular $w k_d \in L(p/q)$ and $k_d \in \operatorname{succ}_{p/q}(w)$. □

A simple induction using Lemma 3.5.4 provides the following corollary.

Corollary 3.5.6. For $p \geq 2q-1$ the subshift $\Xi_{p/q} \cap D_{p,q}^{\mathbb{Z}}$ is an SFT and it is equal to $X_{\mathcal{F}}$ with the collection of forbidden words

$$\mathcal{F} = \Sigma_{pq}^2 \setminus \{ba \in D_{p,q}^2 \mid b \in Q_{q,p}(j_d) \text{ and } a \in Q_{p,q}(k_d) \text{ for some } d \in \Sigma_q\}$$

where $j_d \in \Sigma_q$ is the unique digit with $k_d q = j_d p + d$.

Example 3.5.7. Consider the case $p = 3$ and $q = 2$. Recall that $D_{3,2} = \{0, 2, 3, 5\}$, $k_0 = 0$, $k_1 = 2$ and $j_0 = 0$ and $j_1 = 1$. Then $(Q_{2,3}(j_0) \times Q_{3,2}(k_0)) \cap D_{3,2}^2 = (\{0,2,4\} \times \{0,3\}) \cap D_{3,2}^2 = \{0,2\} \times \{0,3\}$ and $(Q_{2,3}(j_1) \times Q_{3,2}(k_1)) \cap D_{3,2}^2 = (\{1,3,5\} \times \{2,5\}) \cap D_{3,2}^2 = \{3,5\} \times \{2,5\}$. The subshift $\Xi_{3/2} \cap D_{3,2}^{\mathbb{Z}}$ is determined by a collection of forbidden words

$$\mathcal{F} = \Sigma_6^2 \setminus ((\{0,2\} \times \{0,3\}) \cup (\{3,5\} \times \{2,5\})).$$

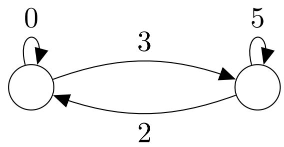

Figure 3.8: The graph of the subshift $\Xi_{3/2} \cap D_{3,2}^{\mathbb{Z}}$.

and its elements are the labels of all bi-infinite paths in the graph in Figure 3.8.

From Figure 3.8 it is clear that $\left|L(3/2) \cap D_{3,2}^n\right| = 2^{n+1}$ for every $n > 0$. This fact can be generalized.

Lemma 3.5.8. If $p \geq 2q - 1$, then $\left|L(p/q) \cap D_{p,q}^n\right| = q^{n+1}$ for every $n > 0$.

Proof. The proof is by induction. The case $n = 1$ is clear because $|D_{p,q}| = q^2$. Next assume that the equality $\left|L(p/q) \cap D_{p,q}^n\right| = q^{n+1}$ holds for some $n > 0$. To prove the induction step, it would be sufficient to show that $\left|\mathrm{pred}_{p/q}(w) \cap D_{p,q}\right| = q$ for every $w \in L(p/q) \cap D_{p,q}^n$. Since $w \in L(p/q) \cap D_{p,q}^n$, it can be written in the form $w = av$ with $a \in D_{p,q}$, $v \in \Sigma_{pq}^*$ and $a \equiv k_d \pmod p$ for some $d \in \Sigma_q$. By Lemma 3.5.4 $\mathrm{pred}_{p/q}(av) = Q_{q,p}(j_d)$ and by Lemma 3.5.3 we have that $|Q_{q,p}(j_d) \cap D_{p,q}| = q$, so we are done. $\square$

Lemma 3.5.9. For any $x \in \Sigma_{pq}^{\mathbb{Z}}$ and $d \in D_{p,q}$ there is a configuration $z \in \Sigma_{pq}^{\mathbb{Z}}$ such that $z[-\infty, 0] = x[-\infty, 0]$, $z[1] = d$ and $\mathrm{Tr}_{p/q,1}(z)[0, \infty] \in D_{p,q}^{\mathbb{N}}$.

Proof. We will show that for every integer $k \geq -1$ there is a configuration $z_k \in \Sigma_{pq}^{\mathbb{Z}}$ such that $z_k[-i] = x[-i]$ for $0 \leq i \leq k$, $z_k[1] = d$ and $\mathrm{Tr}_{p/q,1}(z_k)[0, \infty] \in D_{p,q}^{\mathbb{N}}$. Then the claim of the lemma follows by choosing $z \in \Sigma_{pq}^{\mathbb{Z}}$ as the limit of some converging subsequence of $(z_k)_{k \geq -1}$.

The proof is by induction on k. In case $k = -1$ we take any $w \in \Xi_{p/q} \cap D_{p,q}^{\mathbb{Z}}$ such that $w[0] = d$, which exists by Lemma 3.5.5. The configuration w can be realized as a trace of some configuration $z_{-1} \in \Sigma_{pq}^{\mathbb{Z}}$, i.e. $z_{-1}[1] = d$ and $\mathrm{Tr}_{p/q,1}(z_{-1}) = w \in D_{p,q}^{\mathbb{Z}}$.

Assume now that z_k has been constructed for some $k \geq -1$. Let $z' \in \Sigma_{pq}^{\mathbb{Z}}$ be such that $z'[-(k+1)] = x[-(k+1)]$ and $z'[i] = z_k[i]$ for $i \in \mathbb{Z} \setminus \{-(k+1)\}$. By Proposition 3.3.10 $\Pi_{p/q,pq}^{k+2}(z')[1]$ is congruent to $\Pi_{p/q,pq}^{k+2}(z_k)[1] \in D_{p,q}$ modulo p and therefore $\Pi_{p/q,pq}^{k+2}(z')[1] \in D_{p,q}$. Now choose $w \in \Xi_{p/q} \cap D_{p,q}^{\mathbb{Z}}$ such that $w[i] = \Pi_{p/q,pq}^{i}(z')[1]$ when $0 \leq i \leq k+2$ (this exists by Lemma 3.5.5) and let $y \in \Sigma_{pq}^{\mathbb{Z}}$ such that $\mathrm{Tr}_{p/q,1}(y) = w$. Then define a new configuration z_{k+1} by

$$z_{k+1}[i] = \begin{cases} x[i] = z'[i] & \text{when } -(k+1) \leq i \leq 0 \\ y[i] & \text{when } i > 0 \end{cases}$$

and for other indices i, $z_{k+1}[i]$ will be defined suitably. Now it suffices to prove the following claim.

Claim. It is possible to define $z_{k+1}[-i]$ for $i > k+1$ in such a way that $\mathrm{Tr}_{p/q,1}(z_{k+1})[m] = w[m]$ for all $m \in \mathbb{N}$.

Proof of claim. The proof is by induction on m. The case $m = 0$ is trivial, because $\mathrm{Tr}_{p/q,1}(z_{k+1})[0] = z_{k+1}[1] = y[1] = w[0]$.

Assume next that the claim holds for all natural numbers up to m. To prove the claim for $m+1$, we consider two different cases.

Case $m+1 \leq k+2$: Since $\mathrm{Tr}_{p/q,1}(z_{k+1})[i] = \mathrm{Tr}_{p/q,1}(z')[i]$ for $i \leq m$, from $z_{k+1}[-m, 0] = z'[-m, 0]$ it follows that $\Pi^m_{p/q,pq}(z_{k+1})[0] = \Pi^m_{p/q,pq}(z')[0]$ and from $z_{k+1}[2, \infty] = y[2, \infty]$ it follows that $\Pi^m_{p/q,pq}(z_{k+1})[2] = \Pi^m_{p/q,pq}(y)[2]$. Therefore,

$$
\begin{aligned}
&\mathrm{Tr}_{p/q,1}(z_{k+1})[m+1] \\
&= f_{p/q,pq}(\Pi^m_{p/q,pq}(z_{k+1})[0], \Pi^m_{p/q,pq}(z_{k+1})[1], \Pi^m_{p/q,pq}(z_{k+1})[2]) \\
&= f_{p/q,pq}(\Pi^m_{p/q,pq}(z')[0], w[m], \Pi^m_{p/q,pq}(y)[2]) \\
&= f_{p/q,pq}(\Pi^m_{p/q,pq}(z')[0], \Pi^m_{p/q,pq}(z')[1], \Pi^m_{p/q,pq}(y)[2]) = w[m+1],
\end{aligned}
$$

where the last equality follows from

$$
\begin{aligned}
&f_{p/q,pq}(\Pi^m_{p/q,pq}(z')[0], \Pi^m_{p/q,pq}(z')[1], \Pi^m_{p/q,pq}(z')[2]) = w[m+1] \\
&= f_{p/q,pq}(\Pi^m_{p/q,pq}(y)[0], \Pi^m_{p/q,pq}(z')[1], \Pi^m_{p/q,pq}(y)[2])
\end{aligned}
$$

by applying Corollary 3.3.7.

Case $m+1 > k+2$: As in the previous case we find that the equality $\Pi^m_{p/q,pq}(z_{k+1})[2] = \Pi^m_{p/q,pq}(y)[2]$ holds. By Proposition 3.3.10

$$
\begin{aligned}
&\mathrm{Tr}_{p/q,1}(z_{k+1})[m+1] \\
&= f_{p/q,pq}(\Pi^m_{p/q,pq}(z_{k+1})[0], \Pi^m_{p/q,pq}(z_{k+1})[1], \Pi^m_{p/q,pq}(z_{k+1})[2]) \\
&= f_{p/q,pq}(\Pi^m_{p/q,pq}(z_{k+1})[0], \Pi^m_{p/q,pq}(y)[1], \Pi^m_{p/q,pq}(y)[2])
\end{aligned}
$$

and $w[m+1] = f_{p/q,pq}(\Pi^m_{p/q,pq}(y)[0], \Pi^m_{p/q,pq}(y)[1], \Pi^m_{p/q,pq}(y)[2])$ are congruent modulo p. By Proposition 3.3.10, $z_{k+1}[-m]$ can be chosen such that $\mathrm{Tr}_{p/q,1}(z_{k+1})[m+1] = w[m+1]$. $\square$

Corollary 3.5.10. If $p \geq 2q-1$, then for every $n \in \mathbb{N}$ and $d \in D_{p,q}$ we have $Z_{p/q}(I) \cap \left[n + \frac{1}{pq}d, n + \frac{1}{pq}(d+1)\right] \neq \emptyset$, where

$$
I = \bigcup_{a \in D_{p,q}} \left[\frac{1}{pq}a, \frac{1}{pq}(a+1)\right].
$$

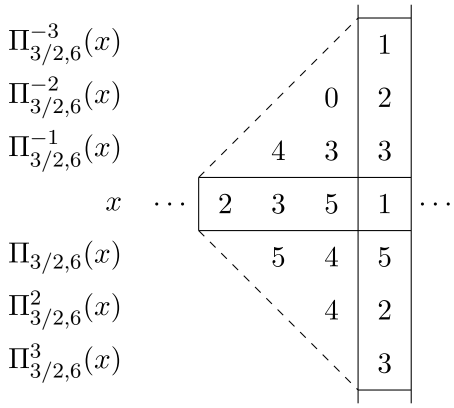

Figure 3.9: A part of the configuration computed from the trace.

Proof. Let $x = \mathrm{config}_{pq}(n)$, let $z \in \Sigma_{pq}^{\mathbb{Z}}$ be as in the statement of the previous lemma and let $\xi = \mathrm{real}(z)$. Then $\xi \in \left[n + \frac{d}{pq}, n + \frac{d+1}{pq}\right]$ and from $\mathrm{Tr}_{p/q,1}(z)[0,\infty] \in D_{p,q}^{\mathbb{N}}$ it follows that $\xi \in Z_{p/q}(I)$. $\square$

Remark 3.5.11. Akiyama, Frougny and Sakarovitch have proved in [1] that if $p \geq 2q - 1$, then $Z_{p/q}(I') \neq \emptyset$, where

$$I' = \bigcup_{d \in \Sigma_q} \left[\frac{1}{p} k_d, \frac{1}{p}(k_d + 1)\right].$$

Their proof is based on the study of a non-stardard base-p/q numeration system. The previous corollary gives a new proof of this fact, because multiplying any element of $Z_{p/q}(I)$ by q yields an element of $Z_{p/q}(I')$.

Theorem 3.5.12. If $p \geq 2q - 1$ and $k > 0$, then there exists a finite union of intervals $I_{p,q,k}$ of total length at most $(q/p)^k$ such that $Z_{p/q}(I_{p,q,k}) \neq \emptyset$.

Proof. Let $k > 0$ be fixed and using Lemma 3.5.9 choose any $x' \in \Sigma_{pq}^{\mathbb{Z}}$ such that $\mathrm{real}(x') > 0$ and $\mathrm{Tr}_{p/q,1}(x) \in D_{p,q}^{\mathbb{N}}$. Let $x = \Pi_{p/q,pq}^{k-1}(\sigma^{-(k-1)}(x'))$ and $\xi = \mathrm{real}(x)$. Based on x we define a collection of words

$$W = \{\Pi_{p/q,pq}^{n}(x)[1,k] \mid n \in \mathbb{N}\}.$$

The set W determines a finite union of intervals

$$I_{p,q,k} = \bigcup_{w \in W} \left[\mathrm{real}_{pq}(w), \mathrm{real}_{pq}(w) + (pq)^{-k}\right],$$

and $\xi \in Z_{p/q}(I_{p,q,k})$ by the definition of W. Each interval in $I_{p,q,k}$ has length $(pq)^{-k}$, so to prove that the total length of $I_{p,q,k}$ is at most $(q/p)^k$ it is sufficient to show that $|W| \leq q^{2k}$.

For the k-trace of x we have

$$\begin{aligned}\mathrm{Tr}_{p/q,k}(x)[i] &= \mathrm{Tr}_{p/q,k}(\Pi^{k-1}_{p/q,pq}(\sigma^{-(k-1)}(x')))[i] \\ &= \mathrm{Tr}_{p/q,1}(\Pi^{k-1}_{p/q,pq}(x'))[i] \\ &= \mathrm{Tr}_{p/q,1}(x')[i+(k-1)] \text{ for every } i \in \mathbb{N},\end{aligned}$$

from which it follows that $\mathrm{Tr}_{p/q,k}(x)[i] \in D_{p,q}$ for every $i \geq -(k-1)$. Thus, the words in the set

$$V = \{\mathrm{Tr}_{p/q,k}(\Pi^n_{p/q,pq}(x))[-(k-1),(k-1)] \mid n \in \mathbb{N}\}$$

belong to $L(p/q) \cap D^{2k-1}_{p,q}$. By using the radius-1 CA $\Delta_{p/q}$ from Proposition 3.3.4 we see that for every n the word $\Pi^n_{p/q,pq}(x)[1,k]$ can be computed from $\mathrm{Tr}_{p/q,k}(\Pi^n_{p/q,pq}(x))[-(k-1),(k-1)]$ (see Figure 3.9) and therefore $|W| \leq |V|$. Combining this observation with Lemma 3.5.8 yields

$$|W| \leq |V| \leq \left|L(p/q) \cap D^{2k-1}_{p,q}\right| = q^{2k}.$$

□

Remark 3.5.13. The set $I_{p,q,k}$ constructed in the proof of the previous theorem is a union of q^{2k} intervals, each of which is of length $(pq)^{-k}$.

Corollary 3.5.14. If $p > q > 1$ and $\epsilon > 0$, then there exists a finite union of intervals $J_{p,q,\epsilon}$ of total length at most ϵ such that $Z_{p/q}(J_{p,q,\epsilon}) \neq \emptyset$.

Proof. Choose some $n > 0$ such that $p^n \geq 2q^n - 1$. Then by the previous theorem there exists a finite union of intervals I_0 of total length at most $\eta = \epsilon(p-1)/(p^n-1)$ such that $Z_{p^n/q^n}(I_0) \neq \emptyset$. For $0 < i < n$ define inductively

$$I_i = \left\{\mathrm{frac}\left(\xi\frac{p}{q}\right) \in [0,1) \,\middle|\, \xi \geq 0 \text{ and } \mathrm{frac}\,(\xi) \in I_{i-1}\right\}.$$

We show by induction that each I_i is a finite union of intervals of total length at most $p^i\eta$. Assume therefore that I_{i-1} has total length at most $p^{i-1}\eta$ and for $0 \leq j < q$ let

$$I_{i,j} = \left\{\mathrm{frac}\left(\xi\frac{p}{q}\right) \in [0,1) \,\middle|\, \xi \geq 0, \lfloor\xi\rfloor \equiv j \pmod q \text{ and } \mathrm{frac}\,(\xi) \in I_{i-1}\right\}.$$

Each $I_{i,j}$ is a finite union of intervals of total length at most $(p/q)p^{i-1}\eta$, because $\mathrm{frac}\left(\xi\frac{p}{q}\right)$ depends only on $\mathrm{frac}(\xi)$ and the value of $\lfloor\xi\rfloor$ modulo q. Then from $I_i = \bigcup_{j=0}^{q-1} I_{i,j}$ it follows that I_i is a finite union of intervals of total length at most $q(p/q)q^{i-1}\eta = p^i\eta$.

We conclude by noting that $J_{p,q,\epsilon} = \bigcup_{i=0}^{n-1} I_i$ is a finite union of intervals of total length at most

$$\sum_{i=0}^{n-1} (p^i)\eta = \frac{p^n - 1}{p - 1}\eta = \epsilon$$

and $Z_{p/q}(J_{p,q,\epsilon}) \supseteq Z_{p^k/q^k}(I_0) \neq \emptyset$. $\square$

3.6 Mixingness of Fractional Multiplication Automata and the Distribution of Fractional Parts $\mathrm{frac}(\xi(p/q)^i)$

In this section we assume that $p, q > 1$ are integers that are not necessarily coprime and that μ is the uniform measure on $\Sigma_{pq}^{\mathbb{Z}}$. We will prove that $\Pi_{p/q,pq}$ is strongly mixing with respect to μ when $p > q$. As a corollary we prove the existence of large sets S such that $Z_{p/q}(S)$ is empty.

The next lemma is a special case of a well known measure theoretical result (see e.g. Theorem 2.18 in [47]):

Lemma 3.6.1. For every $S \in \Sigma(\mathcal{C})$ and $\epsilon > 0$ there is an open set $U \subseteq A^{\mathbb{Z}}$ such that $S \subseteq U$ and $\mu(U \setminus S) < \epsilon$.

Lemma 3.6.2. If $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is an ergodic CA, then for every $\epsilon > 0$ there is a finite collection of cylinders $\{U_i\}_{i \in I}$ such that $\mu(\bigcup_{i \in I} U_i) < \epsilon$ and

$$\left\{ x \in A^{\mathbb{Z}} \;\middle|\; F^t(x) \in \bigcup_{i \in I} U_i \text{ for some } t \in \mathbb{N} \right\} = A^{\mathbb{Z}}.$$

Proof. Let $C \in \mathcal{C}$ be such that $0 < \mu(C) < \epsilon/2$. By continuity of F, $B = \bigcup_{t \in \mathbb{N}} F^{-t}(C)$ is open and $\mu(B) = 1$ by ergodicity of F (see Theorem 1.5 in [59]). Equivalently, $B' = A^{\mathbb{Z}} \setminus B$ is closed (and compact) and $\mu(B') = 0$. Let V be an open set such that $B' \subseteq V$ and $\mu(V) < \epsilon/2$: such a set exists by Lemma 3.6.1. Because $\mathcal{C}$ is a basis of the topology of $A^{\mathbb{Z}}$, there is a collection of cylinders $\{V_i\}_{i \in J}$ such that $V = \bigcup_{i \in J} V_i$. By compactness of B' there is a finite set $I' \subseteq J$ such that $B' \subseteq \bigcup_{i \in I'} V_i$. Now $\{U_i\}_{i \in I} = \{C\} \cup \{V_i\}_{i \in I'}$ is a finite collection of cylinders such that $\mu(\bigcup_{i \in I} U_i) < \epsilon$ and

$$\left\{ x \in A^{\mathbb{Z}} \;\middle|\; F^t(x) \in \bigcup_{i \in I} U_i \text{ for some } t \in \mathbb{N} \right\} \supseteq B \cup \bigcup_{i \in I'} V_i \supseteq B \cup B' = A^{\mathbb{Z}}.$$

$\square$

We will prove that $\Pi_{p/q,pq}$ is strongly mixing. For the statement of the following lemmas, we define a function $\mathrm{int} : \Sigma_{pq}^{+} \to \mathbb{N}$ by

$$\mathrm{int}(w[1]w[2]\cdots w[k]) = \sum_{i=0}^{k-1} w[k-i](pq)^i,$$

i.e. $\mathrm{int}(w)$ is the integer having w as a base-pq representation.

Lemma 3.6.3. Let $w_1, w_2 \in \Sigma_{pq}^k$ for some $k \geq 2$ and let $t > 0$ be a natural number. Then

1. $\mathrm{int}(w_1) < q^t \implies \mathrm{int}(g_{p,pq}(w_1)) < q^{t-1}$ and
2. $\mathrm{int}(w_2) \equiv \mathrm{int}(w_1) + q^t \pmod{(pq)^k}$
   $\implies \mathrm{int}(g_{p,pq}(w_2)) \equiv \mathrm{int}(g_{p,pq}(w_1)) + q^{t-1} \pmod{(pq)^{k-1}}$.

Proof. Let $x_i \in \Sigma_{pq}^{\mathbb{Z}}$ $(i = 1, 2)$ be such that $x_i[-(k-1), 0] = w_i$ and $x_i[j] = 0$ for $j < -(k-1)$ and $j > 0$. From this definition of x_i it follows that $\mathrm{int}(w_i) = \mathrm{real}_{pq}(x_i)$. Denote $y_i = \Pi_{p,pq}(x_i)$. We have

$$\sum_{j=-\infty}^{\infty} y_i[-j](pq)^j = \mathrm{real}_{pq}(y_i) = p\,\mathrm{real}_{pq}(x_i) = p\,\mathrm{int}(w_i)$$

and

$$\begin{aligned}\mathrm{int}(g_{p,pq}(w_i)) &= \mathrm{int}(y_i[-(k-1), -1]) \\ &= \sum_{j=1}^{k-1} y_i[-j](pq)^{j-1} \equiv \lfloor \mathrm{int}(w_i)/q \rfloor \pmod{(pq)^{k-1}}.\end{aligned}$$

Also note that $\mathrm{int}(g_{p,pq}(w_i)) < (pq)^{k-1}$.

For the proof of the first part, assume that $\mathrm{int}(w_1) < q^t$. Combining this with the observations above yields $\mathrm{int}(g_{p,pq}(w_i)) \leq \lfloor \mathrm{int}(w_i)/q \rfloor < q^{t-1}$.

For the proof of the second part, assume that $\mathrm{int}(w_2) \equiv \mathrm{int}(w_1) + q^t \pmod{(pq)^k}$. Then there exists $n \in \mathbb{Z}$ such that $\mathrm{int}(w_2) = \mathrm{int}(w_1) + q^t + n(pq)^k$ and

$$\begin{aligned}\mathrm{int}(g_{p,pq}(w_2)) &\equiv \lfloor \mathrm{int}(w_2)/q \rfloor \equiv \lfloor \mathrm{int}(w_1)/q \rfloor + q^{t-1} + np(pq)^{k-1} \\ &\equiv \lfloor \mathrm{int}(w_1)/q \rfloor + q^{t-1} \equiv \mathrm{int}(g_{p,pq}(w_1)) + q^{t-1} \pmod{(pq)^{k-1}}.\end{aligned}$$

□

Lemma 3.6.4. Let $t > 0$ and $w_1, w_2 \in \Sigma_{pq}^k$ for some $k \geq t + 1$.

1. If $\mathrm{int}(w_1) < q^t$, then $\mathrm{int}(g_{p,pq}^t(w_1)) = 0$.

2. If $\mathrm{int}(w_2) \equiv \mathrm{int}(w_1) + q^t \pmod{(pq)^k}$, then
   $\mathrm{int}(g^t_{p,pq}(w_2)) \equiv \mathrm{int}(g^t_{p,pq}(w_1)) + 1 \pmod{(pq)^{k-t}}$.

Proof. Both claims follow by repeated application of the previous lemma. □

Lemma 3.6.5. Let $t > 0$ and $w_1, w_2 \in \Sigma^k_{pq}$ for some $k \geq 2t + 1$. Then

1. $\mathrm{int}(w_1) < q^{2t} \implies \mathrm{int}(f^t_{p/q,pq}(w_1)) = 0$ and

2. $\mathrm{int}(w_2) \equiv \mathrm{int}(w_1) + q^{2t} \pmod{(pq)^k}$
   $\implies \mathrm{int}(f^t_{p/q,pq}(w_2)) \equiv \mathrm{int}(f^t_{p/q,pq}(w_1)) + 1 \pmod{(pq)^{k-2t}}$.

Proof. Note that $f_{p/q,pq}(w) = g^2_{p,pq}(w)$ for every $w \in \Sigma^*_{pq}$ such that $|w| \geq 3$ by the definition of the local rule $f_{p/q,pq}$. The result therefore follows from the previous lemma. □

The content of Lemma 3.6.5 is as follows. Assume that $\{w_i\}_{i=0}^{(pq)^k-1}$ is the enumeration of all the words in Σ^k_{pq} in the lexicographical order, meaning that $w_0 = 00\cdots00$, $w_1 = 00\cdots01$, $w_2 = 00\cdots02$ and so on. Then let i run through all the integers between 0 and $(pq)^k - 1$. For the first q^{2t} values of i we have $f^t_{p/q,pq}(w_i) = 00\cdots00$, for the next q^{2t} values of i we have $f^t_{p/q,pq}(w_i) = 00\cdots01$, and for the following q^{2t} values of i we have $f^t_{p/q,pq}(w_i) = 00\cdots02$. Eventually, as i is incremented from $q^{2t}(pq)^{k-2t}-1$ to $q^{2t}(pq)^{k-2t}$, the word $f^t_{p/q,pq}(w_i)$ loops from $(pq-1)(pq-1)\cdots(pq-1)(pq-1)$ back to $00\cdots00$.

Theorem 3.6.6. If $p > q > 1$, then $\Pi_{p/q,pq}$ is strongly mixing and in particular ergodic.

Proof. Firstly, $\Pi_{p/q,pq}$ preserves the uniform measure because it is surjective. Then, by Theorem 1.17 in [59] it is sufficient to verify the condition

$$\lim_{t\to\infty} \mu(\Pi^{-t}_{p/q,pq}(C_1) \cap C_2) = \mu(C_1)\mu(C_2)$$

for every $C_1, C_2 \in \mathcal{C}$. Without loss of generality we may consider cylinders $C_1 = \mathrm{Cyl}(v_1, 0)$ and $C_2 = \mathrm{Cyl}(v_2, i)$. Denote $l_1 = |v_1|$, $l_2 = |v_2|$ and let $t \geq i + l_2$ be a natural number.

Consider an arbitrary word $w \in \Sigma^{2t+l_1}_{pq}$ and its decomposition $w = w_1w_2w_3$, where $w_1 \in \Sigma^{t+i}_{pq}$, $w_2 \in \Sigma^{l_2}_{pq}$ and $w_3 \in \Sigma^{t+l_1-i-l_2}_{pq}$. The following conditions may or may not be satisfied by w (see Figure 3.10):

1. $f^t_{p/q,pq}(w) = v_1$

2. $w_2 = v_2$.

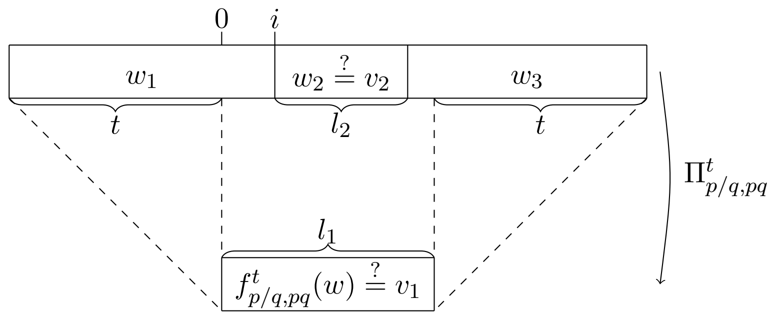

Figure 3.10: Relations between the words v_1, v_2 and $w_1w_2w_3$.

Note that if w satisfies condition 1, then $\Pi^t_{p/q,pq}(\mathrm{Cyl}(w,-t)) \subseteq C_1$, and otherwise $\Pi^t_{p/q,pq}(\mathrm{Cyl}(w,-t)) \cap C_1 = \emptyset$. Also, if w satisfies condition 2, then $\mathrm{Cyl}(w,-t) \subseteq C_2$, and otherwise $\mathrm{Cyl}(w,-t) \cap C_2 = \emptyset$. Let $W_t \subseteq \Sigma_{pq}^{2t+l_1}$ be the collection of those words w that satisfy both conditions. It follows that

$$\mu(\Pi^{-t}_{p/q,pq}(C_1) \cap C_2) = \mu\left(\bigcup_{w\in W_t} \mathrm{Cyl}(w,-t)\right) = |W_t|(pq)^{-(2t+l_1)}.$$

Next, we estimate the number of words $w = w_1w_2w_3$ in W_t. In any case, to satisfy condition 2, w_2 must equal v_2. Then, for any of the $(pq)^{t+i}$ choices of w_1, the number of choices for w_3 that satisfy condition 1 is between $(pq)^{t+l_1-i-l_2}/(pq)^{l_1} - q^{2t}$ and $(pq)^{t+l_1-i-l_2}/(pq)^{l_1} + q^{2t}$ by Lemma 3.6.5 (and the paragraph following it). Thus,

$$\begin{aligned}&\left((pq)^{t-i-l_2} - q^{2t}\right)(pq)^{t+i}(pq)^{-(2t+l_1)} \le \mu(\Pi^{-t}_{p/q,pq}(C_1) \cap C_2)\\ &\le \left((pq)^{t-i-l_2} + q^{2t}\right)(pq)^{t+i}(pq)^{-(2t+l_1)},\end{aligned}$$

and as t tends to infinity,

$$\lim_{t\to\infty} \mu(\Pi^{-t}_{p/q,pq}(C_1) \cap C_2) = (pq)^{-l_1-l_2} = \mu(C_1)\mu(C_2).$$

□

Remark 3.6.7. One consequence of the map $\Pi_{p/q,pq}$ being ergodic is that $\{\Pi^t_{p/q,pq}(x) \mid t \in \mathbb{N}\}$ is dense in $\Sigma^{\mathbb{Z}}_{pq}$ for almost all $x \in \Sigma^{\mathbb{Z}}_{pq}$. Note the relation with Problem 3.1.10: $\Pi_{p/q,pq}$ being a strongly universal pattern generator with a finite configuration $x \in \Sigma_{pq}$ is equivalent to saying that $\{\Pi^t_{p/q,pq}(x) \mid t \in \mathbb{N}\}$ is dense in $\Sigma^{\mathbb{Z}}_{pq}$.

Theorem 3.6.8. If $p > q > 1$ and $\epsilon > 0$, then there exists a finite union of intervals $K_{p,q,\epsilon} \subseteq [0,1)$ of total length at least $1-\epsilon$ such that $Z_{p/q}(K_{p,q,\epsilon}) = \emptyset$.

Proof. By the previous theorem $\Pi_{p/q,pq}$ is ergodic and by Lemma 3.6.2 there is a finite collection of cylinders $\{U_i\}_{i\in I}$ such that $\mu(\bigcup_{i\in I} U_i) < \epsilon$ and

$$\left\{ x \in \Sigma_{pq}^{\mathbb{Z}} \;\middle|\; \Pi_{p/q,pq}^{t}(x) \in \bigcup_{i\in I} U_i \text{ for some } t \in \mathbb{N} \right\} = \Sigma_{pq}^{\mathbb{Z}}.$$

Without loss of generality we may assume that for every $i \in I$, $U_i = \mathrm{Cyl}(w_i, 1)$ and $w_i \in \Sigma_{pq}^{k}$ for a fixed $k > 0$. Consider the collection of words $W = \Sigma_{pq}^{k} \setminus \{w_i\}_{i\in I}$ and define

$$K_{p,q,\epsilon} = \bigcup_{v\in W} \left[\mathrm{real}_{pq}(v), \mathrm{real}_{pq}(v) + (pq)^{-k}\right).$$

The set $K_{p,q,\epsilon}$ has total length

$$\frac{|W|}{(pq)^k} = 1 - \frac{|I|}{(pq)^k} = 1 - \mu\left(\bigcup_{i\in I} U_i\right) \geq 1 - \epsilon.$$

Now let $\xi > 0$ be arbitrary and denote $x = \mathrm{config}_{pq}(\xi)$. There exists a $t \in \mathbb{N}$ such that $\Pi_{p/q,pq}^{t}(x) \in \bigcup_{i\in I} U_i$, and equivalently, $\Pi_{p/q,pq}^{t}(x) \notin \bigcup_{v\in W}(\mathrm{Cyl}(v,1))$. This means that $\mathrm{frac}(\xi(p/q)^t) \notin K_{p,q,\epsilon}$, and therefore $Z_{p/q}(K_{p,q,\epsilon}) = \emptyset$. □

We conclude this section with one more note on Theorem 3.6.6. It was shown in [56] that if a cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is either left permutive with memory $\neq 0$ or right permutive with anticipation $\neq 0$, then it is strongly mixing. In the proof of Theorem 3.6.6 we used Lemma 3.6.5, which says that $\Pi_{p/q,pq}$ is right permutive in some weaker sense.

Problem 3.6.9. How should one define the class $\mathcal{C}_{\mathrm{wp}} \subseteq \mathrm{End}(A^{\mathbb{Z}})$ of *weak permutive* cellular automata? We want a natural definition such that $\mathcal{C}_{\mathrm{wp}}$ contains all permutive cellular automata as a proper subset and that the elements of $\mathcal{C}_{\mathrm{wp}}$ are strongly mixing with a proof analogous to the proof of Theorem 3.6.6.

3.7 The Lyapunov Exponents of Multiplication Automata

In this section let $p, q > 1$ be coprime integers. We consider the Lyapunov exponents of the multiplication automaton $\Pi_{p,pq}$. Since $\Pi_{p,pq}$ has memory 0 and anticipation 1, it is easy to see that for any $n \in \mathbb{N}$ and $x \in \Sigma_{pq}^{\mathbb{Z}}$ we must have $\lambda^+(x) = 0$ and $\lambda^-(x) \leq 1$ and therefore $\lambda^+ = 0$, $\lambda^- \leq 1$.

Now consider a positive integer $m > 0$. Multiplying m by p^n yields a number whose base-pq representation has length approximately equal to $\log_{pq}(mp^n) = n(\log_{pq} p) + \log_{pq} m$. By translating this observation to the configuration space $\Sigma_{pq}^{\mathbb{Z}}$ it follows that $\lambda^-(0^{\mathbb{Z}}, \Pi_{p,pq}) = \log_{pq} p$. One might be tempted to conclude from this that $\lambda^-(\Pi_{p,pq}) = \log_{pq} p$. It turns out that this conclusion is not true.

Theorem 3.7.1. For coprime $p, q > 1$ there is a configuration $x \in \Sigma_{pq}^{\mathbb{Z}}$ such that $\lambda^-(x, \Pi_{p,pq}) = 1$. In particular $\lambda^-(\Pi_{p,pq}) = 1$.

Proof. For every $n \in \mathbb{N}_+$ define $x_n = \mathrm{config}_{pq}(q^n - 1)$ and $y_n = \mathrm{config}_{pq}(q^n)$. By Lemma 3.1.2, $\mathrm{real}(\Pi_{p,pq}^n(x_n)) = p^n(q^n - 1) < (pq)^n$ and $\mathrm{real}(\Pi_{p,pq}^n(y_n)) = p^n q^n = (pq)^n$, which means that $\Pi_{p,pq}^n(x_n)[-n] = 0$ and $\Pi_{p,pq}^n(y_n)[-n] = 1$. Since $\Pi_{p,pq}$ has memory 0 and anticipation 1, it follows that $\Pi_{p,pq}^i(x_n)[-i] \neq \Pi_{p,pq}^i(y_n)[-i]$ when $0 \leq i \leq n$ (note that q^n isn't divisible by pq for any $n \in \mathbb{N}_+$, which means that x_n and y_n differ only at the origin). Then choose $x, y \in \Sigma_{pq}^{\mathbb{Z}}$ such that $(x, y) \in \Sigma_{pq}^{\mathbb{Z}} \times \Sigma_{pq}^{\mathbb{Z}}$ is the limit of some converging subsequence of $((x_n, y_n))_{n \in \mathbb{N}_+}$. Then x and y differ only at the origin and $\Pi_{p,pq}^i(x)[-i] \neq \Pi_{p,pq}^i(y)[-i]$ for all $i \in \mathbb{N}$. It follows that $\lambda^-(x, \Pi_{p,pq}) = 1$. $\square$

The intuition that the left Lyapunov exponent of $\Pi_{p,pq}$ "should be" equal to $\log_{pq} p$ is explained by the following computation of the average Lyapunov exponent.

Theorem 3.7.2. For coprime $p, q > 1$ we have $I_\mu^-(\Pi_{p,pq}) = \log_{pq} p$, where μ is the uniform measure on $\Sigma_{pq}^{\mathbb{Z}}$.

Proof. First note that for any $n \in \mathbb{N}_+$ and any $w \in \Sigma^{n+1}$ the equality $\Lambda_n^-(x) = \Lambda_n^-(y)$ holds for each pair $x, y \in \mathrm{Cyl}(w, 0)$, so we may define the quantity $\Lambda_n^-(w) = \Lambda_n^-(x)$ for $x \in \mathrm{Cyl}(w, 0)$. For any $i \in \mathbb{N}$ denote $(\Lambda_n^-)^{-1}(i) = \{x \in \Sigma_{pq}^{\mathbb{Z}} \mid \Lambda_n^-(x) = i\}$. Then, note that always $\Lambda_n^-(x) \leq n$ and define for $0 \leq i \leq n$

$$P_n(i) = \{w \in \Sigma_{pq}^{n+1} \mid \Lambda_n^-(w) = i\}$$

which form a partition of Σ_{pq}^{n+1}. From these definitions it follows that

$$I_{n,\mu}^- = \int_{x \in \Sigma_{pq}^{\mathbb{Z}}} \Lambda_n^-(x) d\mu = \sum_{i=0}^{\infty} i\mu((\Lambda_n^-)^{-1}(i)) = (pq)^{-(n+1)} \sum_{i=0}^{n} i|P_n(i)|.$$

To compute $|P_n(i)|$ we define an auxiliary quantity

$$p_n(i) = \{w \in \Sigma_{pq}^{n+1} \mid i \leq \Lambda_n^-(w) \leq n\} :$$

then clearly $P_n(n) = p_n(n)$ and $P_n(i) = p_n(i) \setminus p_n(i+1)$ for $0 \le i < n$. Note that $w \in p_n(i)$ $(0 \le i \le n)$ is equivalent to the existence of words $u \in \Sigma_{pq}^i$, $v_1, v_2 \in \Sigma_{pq}^{n+1-i}$ such that $w = uv_1$ and $g_{p,pq}^t(uv_1)[1] \ne g_{p,pq}^t(uv_2)[1]$ for some $i \le t \le n$. By denoting

$$d_n(i) = \{u \in \Sigma_{pq}^i \mid \exists v_1, v_2 \in A^{n+1-i}, t \in [i,n] : g_{p,pq}^t(uv_1)[1] \ne g_{p,pq}^t(uv_2)[1]\},$$

it follows that $|p_n(i)| = (pq)^{n+1-i}|d_n(i)|$. By Lemma 3.6.4, for a word $u \in \Sigma_{pq}^i$ the condition $u \in d_n(i)$ is equivalent to the existence of a number divisible by q^t on the open interval $J(u)_t = (\mathrm{int}(u)(pq)^{t+1-i}, (\mathrm{int}(u)+1)(pq)^{t+1-i})$ for some $t \in [i,n]$. Furthermore, if an integer m is divisible by q^t and $m \in J(u)_t$, then $m(pq)^{n-t} \in J(u)_n$ is divisible by q^n. Thus it is sufficient to consider only the interval $J(u)_n$. We use this to compute $|d_n(i)|$.

In the case $(pq)^{n+1-i} > q^n$ (equivalently: $n \log_{pq} q + i < n+1$) each interval $J(u)_n$ contains a number divisible by q^n and therefore $|d_n(i)| = (pq)^i$.

In the case $(pq)^{n+1-i} < q^n$ (equivalently: $n \log_{pq} q + i > n+1$) each interval $J(u)_n$ contains at most one number divisible by q^n. Then $|d_n(i)|$ equals the number of elements on the interval $[0, (pq)^{n+1})$ which are divisible by q^n but not divisible by $(pq)^{n+1-i}$. Divisibility by both q^n and $(pq)^{n+1-i}$ is equivalent to divisibility by $q^n p^{n+1-i}$ because p and q are coprime. Therefore $|d_n(i)| = (pq)^{n+1}/q^n - (pq)^{n+1}/(q^n p^{n+1-i}) = (pq)p^n - qp^i$.

Let us denote $\kappa = \left\lfloor n - n\log_{pq} q + 1 \right\rfloor$. We can see that when $i < \kappa$,

$$\begin{aligned} |P_n(i)| &= |p_n(i)| - |p_n(i+1)| = (pq)^{n+1-i}|d_n(i)| - (pq)^{n-i}|d_n(i+1)| \\ &= (pq)^{n+1} - (pq)^{n+1} = 0. \end{aligned}$$

We may compute

$$\begin{aligned} (pq)^{n+1} I_{n,\mu}^- &= \sum_{i=0}^{\kappa-1} i|P_n(i)| + \sum_{i=\kappa}^{n} i|P_n(i)| \\ &= n|p_n(n)| + \sum_{i=\kappa}^{n-1} i(|p_n(i)| - |p_n(i+1)|) = \kappa|p_n(\kappa)| + \sum_{i=\kappa+1}^{n} |p_n(i)|, \end{aligned}$$

in which

$$\kappa|p_n(\kappa)| = \kappa(pq)^{n+1-\kappa}|d_n(\kappa)| = \kappa(pq)^{n+1-\kappa}(pq)^{\kappa} = \kappa(pq)^{n+1}$$

and

$$\sum_{i=\kappa+1}^{n} |p_n(i)| = \sum_{i=\kappa+1}^{n} (pq)^{n+1-i}|d_n(i)| = \sum_{i=\kappa+1}^{n} (pq)^{n+1-i}((pq)p^n - qp^i)$$
$$= (pq)p^n \sum_{i=\kappa+1}^{n} (pq)^{n+1-i} - q(pq)^{n+1} \sum_{i=\kappa+1}^{n} q^{-i} \leq (pq)p^n(pq)^{n-\kappa} \sum_{i=0}^{\infty}(pq)^{-i}$$
$$\leq 2(pq)p^n(pq)^{n-(n-n\log_{pq} q+1)+1} \leq 2(pq)p^n(pq)^{\log_{pq} q^n} = 2(pq)^{n+1}.$$

Finally, the left average Lyapunov exponent is

$$I_\mu^- = \lim_{n\to\infty} \frac{I_{n,\mu}^-}{n} = \lim_{n\to\infty} \frac{\kappa|p_n(\kappa)|}{(pq)^{n+1}n} + \lim_{n\to\infty} \frac{\sum_{i=\kappa+1}^{n} |p_n(i)|}{(pq)^{n+1}n} = \lim_{n\to\infty} \frac{\kappa}{n}$$
$$= 1 - \log_{pq} q = \log_{pq} p.$$

□

Remark 3.7.3. We believe that $I_\mu^-(\Pi_{\alpha,n}) = \log_n \alpha$ for all $\alpha \geq 1$ and all natural numbers $n > 1$ such that $\Pi_{\alpha,n}$ is defined (when μ is the uniform measure of $\Sigma_n^{\mathbb{Z}}$). Replacing the application of Lemma 3.6.4 by an application of Lemma 3.6.5 probably yields the result for $\Pi_{p/q,pq}$ when $p > q > 1$ are coprime. A unified approach to cover the general case would be desirable.

3.8 Summary

We conclude this chapter by highlighting the main results, this time without the clutter of intermediary lemmas.

We computed the complexity of the trace subshift $\Xi(\Pi_{p/q,pq})$ in Theorem 3.4.15.

Theorem. $P_{\Xi(\Pi_{p/q,pq})}(n) = pq(p^{n-1} - q^{n-1})\frac{q-1}{p-q} + p^n q$ for every $n \in \mathbb{N}_+$ and for coprime $p > q > 1$.

From a combinatorial point of view it is interesting that this quantity has a reasonably simple closed-form expression. From a dynamical point of view this is less significant because the complexity function of a subshift is not invariant under topological conjugacy. A dynamically more relevant result is proved in Corollary 3.4.19, which says that $\Pi_{p/q,pq}$ has non-sofic subshift factors.

Theorem. If $p > q > 1$ are coprime, then the subshift $\Xi(\Pi_{p/q,pq})$ is not sofic. In particular, the CA $\Pi_{p/q,pq}$ is not regular.

In Theorems 3.6.6 and 3.7.2 we proved results concerning the complexity of measurable dynamics for some classes of multiplication automata.

Theorem. If $p > q > 1$, then $\Pi_{p/q,pq}$ is strongly mixing and in particular ergodic.

Theorem. If $p, q > 1$ are coprime, then $I_\mu^-(\Pi_{p,pq}) = \log_{pq} p$, where μ is the uniform measure on $\Sigma_{pq}^{\mathbb{Z}}$.

As an application of the study of the multiplication automata $\Pi_{p/q,pq}$ multiplying by fractions p/q we proved results related to Mahler's problem in Corollary 3.5.14 and Theorem 3.6.8. These are in some sense dual to each other.

Theorem. If $p > q > 1$ and $\epsilon > 0$, then there exists a finite union of intervals $J_{p,q,\epsilon}$ of total length at most ϵ such that $Z_{p/q}(J_{p,q,\epsilon}) \neq \emptyset$.

Theorem. If $p > q > 1$ and $\epsilon > 0$, then there exists a finite union of intervals $K_{p,q,\epsilon} \subseteq [0, 1)$ of total length at least $1 - \epsilon$ such that $Z_{p/q}(K_{p,q,\epsilon}) = \emptyset$.

Chapter 4

The Lyapunov Exponents of Reversible Cellular Automata are Uncomputable.

We noted in Chapter 2 that the Lyapunov exponents tell how quickly information can propagate in different directions under applying a given CA F. They are a measure of dynamical complexity of F and can for example be used to give an upper bound for the topological entropy of F [57]. In [13] a closed formula for the Lyapunov exponents of linear one-dimensional cellular automata is given, which is a first step in determining for which classes of CA the Lyapunov exponents are computable. It is previously known that the entropy of one-dimensional cellular automata is uncomputable [26] (and furthermore from [22] it follows that there exists a single cellular automaton whose entropy is uncomputable), which gives reason to suspect that also the Lyapunov exponents are uncomputable in general.

The uncomputability of Lyapunov exponents is easy to prove for (not necessarily reversible) cellular automata by using the result from [30] which says that nilpotency of cellular automata with a spreading state is undecidable. We will prove the more specific claim that the Lyapunov exponents are uncomputable even for reversible cellular automata. In the context of proving undecidability results for reversible CA one cannot utilize undecidability of nilpotency for non-reversible CA. An analogous decision problem, the (local) immortality problem, has been used to prove undecidability results for reversible CA [44]. We will use in our proof the undecidability of a variant of the immortality problem, which in turn follows from the undecidability of the tiling problem for 2-way deterministic tile sets.

4.1 Tilings and Undecidability

In this section we recall the well-known connection between cellular automata and tilings on the plane. We use this connection to prove an auxiliary undecidability result for reversible cellular automata.

Definition 4.1.1. A *Wang tile* is formally a function $t : \{N, E, S, W\} \to C$ whose value at I is denoted by t_I. Informally, a Wang tile t should be interpreted as a unit square with edges colored by elements of C. The edges are called *north*, *east*, *south* and *west* in the natural way, and the colors in these edges of t are t_N, t_E, t_S and t_W respectively. A *tile set* is a finite collection of Wang tiles.

Definition 4.1.2. A tiling over a tile set T is a function $\eta \in T^{\mathbb{Z}^2}$ which assigns a tile to every integer point of the plane. A tiling η is said to be valid if neighboring tiles always have matching colors in their edges, i.e. for every $(i, j) \in \mathbb{Z}^2$ we have $\eta(i, j)_N = \eta(i, j+1)_S$ and $\eta(i, j)_E = \eta(i+1, j)_W$. If there is a valid tiling over T, we say that T *admits* a valid tiling.

We say that a tile set T is NE-deterministic if for every pair of tiles $t, s \in T$ the equalities $t_N = s_N$ and $t_E = s_E$ imply $t = s$, i.e. a tile is determined uniquely by its north and east edge. A SW-deterministic tile set is defined similarly. If T is both NE-deterministic and SW-deterministic, it is said to be *2-way deterministic*.

The *tiling problem* is the problem of determining whether a given tile set T admits a valid tiling.

Theorem 4.1.3. [44, Theorem 4.2.1] The tiling problem is undecidable for 2-way deterministic tile sets.

Definition 4.1.4. Let T be a 2-way deterministic tile set and C the collection of all colors which appear in some edge of some tile of T. T is *complete* if for each pair $(a, b) \in C^2$ there exist (unique) tiles $t, s \in T$ such that $(t_N, t_E) = (a, b)$ and $(s_S, s_W) = (a, b)$.

A 2-way deterministic tile set T can be used to construct a complete tile set. Namely, let C be the set of colors which appear in tiles of T, let $X \subseteq C \times C$ be the set of pairs of colors which do not appear in the northeast of any tile and let $Y \subseteq C \times C$ be the set of pairs of colors which do not appear in the southwest of any tile. Since T is 2-way deterministic, there is a bijection $p : X \to Y$. Let $T^{\complement}$ be the set of tiles formed by matching the northeast corners X with the southwest corners Y via the bijection p. Then the tile set $A = T \cup T^{\complement}$ is complete.

Every complete 2-way deterministic tile set A determines a local rule $f : A^2 \to A$ defined by $f(a, b) = c \in A$, where c is the unique tile such that

$a_S = c_N$ and $b_W = c_E$. This then determines a reversible CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ with memory 0 by $F(x)[i] = f(x[i], x[i+1])$ for $x \in A^{\mathbb{Z}}$, $i \in \mathbb{Z}$. The space-time diagram of a configuration $x \in A^{\mathbb{Z}}$ corresponds to a valid tiling η via $\theta(i, -j) = F^j(x)[i] = \eta(i, -i-j)$, i.e. configurations $F^j(x)$ are diagonals of η going from northwest to southeast and the diagonal corresponding to $F^{j+1}(x)$ is below the diagonal corresponding to $F^j(x)$.

Definition 4.1.5. A cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is (p, q)-locally immortal ($p, q \in \mathbb{N}$) with respect to a subset $B \subseteq A$ if there exists a configuration $x \in A^{\mathbb{Z}}$ such that $F^{iq+j}(x)[ip] \in B$ for all $i \in \mathbb{Z}$ and $0 \leq j \leq q$. Such a configuration x is a (p, q)-witness.

Generalizing the definition in [44], we call the following decision problem the (p, q)-*local immortality problem*: given a reversible CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ and a subset $B \subseteq A$, find whether F is (p, q)-locally immortal with respect to B.

Theorem 4.1.6. [44, Theorem 5.1.5] The $(0, 1)$-local immortality problem is undecidable for reversible CA.

We now adapt the proof of Theorem 4.1.6 to get the following result, which we will use in the proof of Theorem 4.2.1.

Lemma 4.1.7. The $(1, 5)$-local immortality problem is undecidable for reversible radius-$\frac{1}{2}$ CA.

Proof. We will reduce the problem of Theorem 4.1.3 to the $(1, 5)$-local immortality problem. Let T be a 2-way deterministic tile set and construct a complete tile set $T \cup T^{\complement}$ as indicated above. Then also $A_1 = (T \times T_1) \cup (T^{\complement} \times T_2)$ (T_1 and T_2 as in Figure 4.1) is a complete tile set.[1] We denote the blank tile of the set T_1 by t_b and call the elements of $R = A_1 \setminus (T \times \{t_b\})$ arrow tiles. As indicated above, the tile set A_1 determines a reversible radius-$\frac{1}{2}$ CA $G_1 : A_1^{\mathbb{Z}} \to A_1^{\mathbb{Z}}$.

Let $A_2 = \{0, 1, 2\}$. Define $A = A_1 \times A_2$ and natural projections $\pi_i : A \to A_i$, $\pi_i(a_1, a_2) = a_i$ for $i \in \{1, 2\}$. By extension we say that $a \in A$ is an arrow tile if $\pi_1(a) \in R$. Let $G : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be defined by $G(c, e) = (G_1(c), e)$ where $c \in A_1^{\mathbb{Z}}$ and $e \in A_2^{\mathbb{Z}}$, i.e. G simulates G_1 in the upper layer. We construct involutive CA J_1, J_2 and H of memory 0 with local rules $j_1 : A_2 \to A_2$,

[1] The arrow markings are used as a shorthand for some coloring such that the heads and tails of the arrows in neighboring tiles match in a valid tiling.

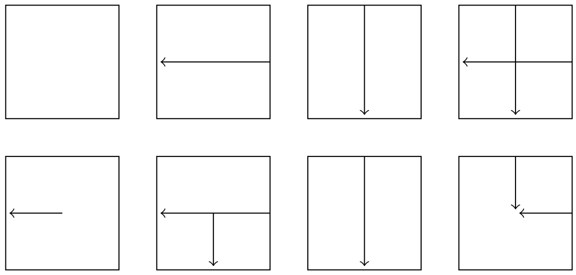

Figure 4.1: The tile sets T_1 (first row) and T_2 (second row). These are originally from [44] (up to a reflection with respect to the northwest - southeast diagonal).

$j_2 : A_2^2 \to A_2$ and $h : (A_1 \times A_2) \to (A_1 \times A_2)$ respectively defined by

$$\begin{array}{ll} j_1(0) = 0 & \\ j_1(1) = 2 & j_2(a,b) = \begin{cases} 1 \text{ when } (a,b) = (0,2) \\ 0 \text{ when } (a,b) = (1,2) \\ a \text{ otherwise} \end{cases} \\ j_1(2) = 1 & \end{array}$$

$$h((a,b)) = \begin{cases} (a,1) \text{ when } a \in R \text{ and } b = 0 \\ (a,0) \text{ when } a \in R \text{ and } b = 1 \\ (a,b) \text{ otherwise.} \end{cases}$$

If $\mathrm{Id} : A_1^{\mathbb{Z}} \to A_1^{\mathbb{Z}}$ is the identity map, then $J = (\mathrm{Id} \times J_2) \circ (\mathrm{Id} \times J_1)$ is a CA on $A^{\mathbb{Z}} = (A_1 \times A_2)^{\mathbb{Z}}$. We define the radius-$\frac{1}{2}$ automaton $F = H \circ J \circ G : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ and select $B = (T \times \{t_b\}) \times \{0\}$. We will show that T admits a valid tiling if and only if F is $(1,5)$-locally immortal with respect to B.

Assume first that T admits a valid tiling η. Then by choosing $x \in A^{\mathbb{Z}}$ such that $x[i] = ((\eta(i,-i), t_b), 0) \in A_1 \times A_2$ for $i \in \mathbb{Z}$ it follows that $F^j(x)[i] \in B$ for all $i, j \in \mathbb{Z}$ and in particular that x is a $(1,5)$-witness.

Assume then that T does not admit any valid tiling and for a contradiction assume that x is a $(1,5)$-witness. Let θ be the space-time diagram of x with respect to F. Since x is a $(1,5)$-witness, it follows that $\theta(i,-j) \in B$ whenever $(i,-j) \in N$, where $N = \{(i,-j) \in \mathbb{Z}^2 \mid 5i \leq j \leq 5(i+1)\}$. There is a valid tiling η over A_1 such that $\pi_1(\theta(i,j)) = \eta(i, j-i)$ for $(i,j) \in \mathbb{Z}^2$, i.e. η can be recovered from the upper layer of θ by applying a suitable linear transformation on the space-time diagram. In drawing pictorial representations of θ we want that the heads and tails of all arrows remain properly matched in neighboring coordinates, so we will use tiles with "bent" labelings, see Figure 4.2. Since T does not admit valid tilings, it follows by a compactness argument that $\eta(i,j) \notin T \times T_1$ for some $(i,j) \in D$ where $D = \{(i,j) \in \mathbb{Z}^2 \mid j > -6i\}$ and in particular that $\eta(i,j)$ is an arrow tile. Since θ contains a "bent" version of η, it follows that $\theta(i,j)$ is an arrow tile for some $(i,j) \in E$, where $E = \{(i,j) \in \mathbb{Z}^2 \mid j > -5i\}$ is a "bent" version of the set D. In Figure 4.3 we present the space-time diagram θ with arrow markings of tiles from T_1 and T_2 replaced according to the Figure 4.2. In Figure 4.3 we have also marked the sets N and E. Other features of the figure become relevant in the next paragraph.

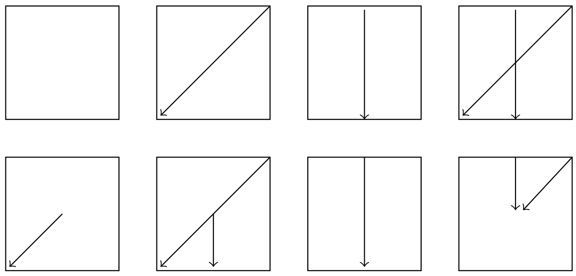

Figure 4.2: The tile sets T_1 and T_2 presented in a “bent” form.

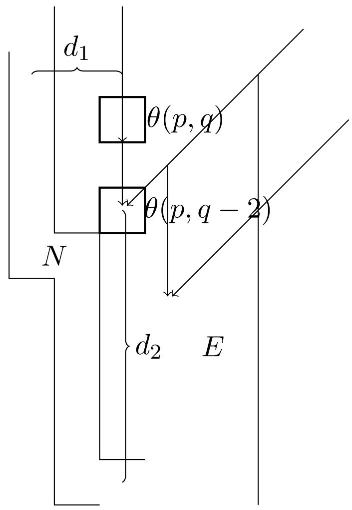

Figure 4.3: The space-time diagram θ with “bent” arrow markings. An arrow tile $\theta(p, q-2)$ in E with minimal horizontal and vertical distances to N has been highlighted.

The minimal distance between a tile in N and an arrow tile in E situated on the same horizontal line in θ is denoted by $d_1 > 0$. Then, among those arrow tiles in E at horizontal distance d_1 from N, there is a tile with minimal vertical distance $d_2 > 0$ from N (see Figure 4.3). Fix $p, q \in \mathbb{Z}$ so that $\theta(p, q-2)$ is one such tile and in particular $(p-d_1, q-2), (p, q-2-d_2) \in N$. Then $\theta(p, q-j)$ contains an arrow for $-2 \leq j \leq 2$, because if there is a $j \in [-2, 2)$ such that $\theta(p, q-j)$ does not contain an arrow and $\theta(p, q-j-1)$ does, then $\theta(p, q-j-1)$ must contain one of the three arrows on the left half of Figure 4.2. These three arrows continue to the southwest, so then also

$\theta(p-1,q-j-2)$ contains an arrow. Because $\theta(p',q') \in B$ for $(p',q') \in N$, it follows that $(p-1,q-j-2) \notin N$ and thus $(p-1,q-j-2) \in E$. Since $(p-d_1,q-2) \in N$, it follows that one of the $(p-d_1-1,q-j-2)$, $(p-d_1,q-j-2)$ and $(p-d_1+1,q-j-2)$ belong to N. Thus the horizontal distance of the tile $\theta(p-1,q-j-2)$ from the set N is at most d_1, and is actually equal to d_1 by the minimality of d_1. Since N is invariant under translation by the vector $-(1,-5)$, then from $(p,q-2-d_2) \in N$ it follows that $(p-1,q+3-d_2) \in N$ and that the vertical distance of the tile $\theta(p-1,q-j-2)$ from N is at most $(q-j-2)-(q+3-d_2) \leq d_2-3$, contradicting the minimality of d_2. Similarly, $\theta(p-i,q-j)$ does not contain an arrow for $0 < i \leq d_1$, $-2 \leq j \leq 2$ by the minimality of d_1 and d_2.

Now consider the A_2-layer of θ. For the rest of the proof let $y = F^{-q}(x)$. Assume that $\pi_2(\theta(p-i,q)) = \pi_2(y[p-i])$ is non-zero for some $i \geq 0$, $(p-i,q) \in E$, and fix the greatest such i, i.e. $\pi_2(y[s]) = 0$ for s in the set

$$I_0 = \{p' \in \mathbb{Z} \mid p' < p-i, (p',q) \in N \cup E\}.$$

We start by considering the case $\pi_2(y[p-i]) = 1$. Denote

$$I_1 = \{p' \in \mathbb{Z} \mid p' < p-i, (p',q-1) \in N \cup E\} \subseteq I_0.$$

From the choice of (p,q) it follows that $\pi_1(\theta(s,q-1)) = \pi_1(G(y)[s])$ are not arrow tiles for $s \in I_1$, and therefore we can compute step by step that

$$\begin{aligned}
&\pi_2((\mathrm{Id} \times J_1)(G(y))[p-i]) = 2, \quad \pi_2((\mathrm{Id} \times J_1)(G(y))[s]) = 0 \text{ for } s \in I_0 \subseteq I_1, \\
&\pi_2(J(G(y))[p-(i+1)]) = 1, \quad \pi_2(J(G(y))[s]) = 0 \text{ for } s \in I_1 \setminus \{p-(i+1)\}, \\
&\pi_2(F(y))[p-(i+1)]) = 1, \quad \pi_2(F(y)[s]) = 0 \text{ for } s \in I_1 \setminus \{p-(i+1)\}
\end{aligned}$$

and $\pi_2(\theta(p-(i+1),q-1)) = 1$. By repeating this argument inductively we see that the digit 1 propagates to the lower left in the space-time diagram as indicated by Figure 4.4 and eventually reaches N, a contradiction. If on the other hand $\pi_2(\theta(p-i,q)) = 2$, a similar argument shows that the digit 2 propagates to the upper left in the space-time diagram as indicated by Figure 4.4 and eventually reaches N, also a contradiction.

Assume then that $\pi_2(\theta(p-i,q))$ is zero whenever $i \geq 0$, $(p-i,q) \in E$. If $\pi_2(\theta(p+1,q)) = \pi_2(y[p+1]) \neq 1$, then $\pi_2((\mathrm{Id} \times J_1)(G(y))[p+1]) \neq 2$ and $\pi_2(J(G(y))[p]) = 0$. Since $\pi_1(\theta(p,q-1))$ is an arrow tile, it follows that $\pi_2(\theta(p,q-1)) = \pi_2(H(J(G(y)))[p]) = 1$. The argument of the previous paragraph shows that the digit 1 propagates to the lower left in the space-time diagram as indicated by the left side of Figure 4.5 and eventually reaches N, a contradiction.

Finally consider the case $\pi_2(\theta(p+1,q)) = \pi_2(y[p+1]) = 1$. Then

$$\begin{aligned}
&\pi_2(J(G(y))[p])\pi_2(J(G(y))[p+1]) = 12 \text{ and} \\
&\pi_2(F(y)[p])\pi_2(F(y)[p+1]) = 02.
\end{aligned}$$

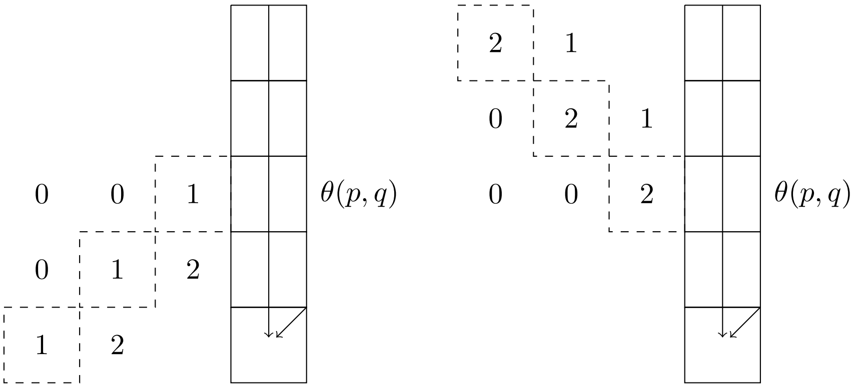

Figure 4.4: Propagation of digits to the left of $\theta(p, q)$.

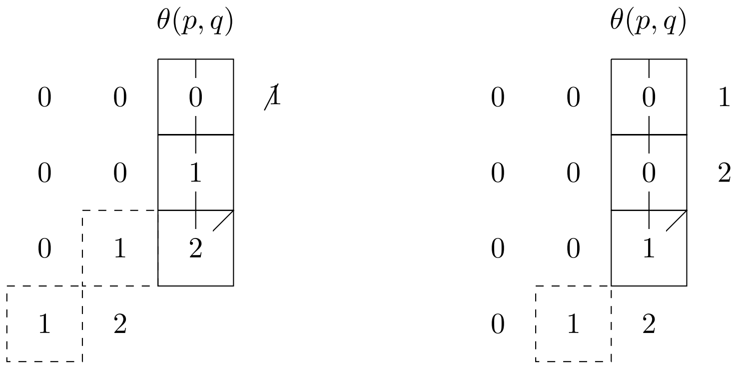

Figure 4.5: Propagation of digits at $\theta(p, q)$.

As in the previous paragraph we see that $\pi_2(\theta(p, q-2)) = 1$. This occurrence of the digit 1 propagates to the lower left in the space-time diagram as indicated by the right side of Figure 4.5 and eventually reaches N, a contradiction.

$\square$

Remark 4.1.8. It is possible that the (p, q)-local immortality problem is undecidable for reversible radius-$\frac{1}{2}$ CA whenever $p \in \mathbb{N}$ and $q \in \mathbb{N}_+$. We proved this in the case $(p, q) = (1, 5)$ but for our purposes it is sufficient to prove this just for some $p > 0$ and $q > 0$. The important (seemingly paradoxical) part will be that for $(1, 5)$-locally immortal radius-$\frac{1}{2}$ CA F the "local immortality" travels to the right in the space-time diagram even though in reality there cannot be any information flow to the right because F is one-sided.

4.2 Uncomputability of Lyapunov exponents

In this section we will prove the main result of this chapter saying that there is no algorithm that can compute the Lyapunov exponents of a given reversible cellular automaton on a full shift to an arbitrary precision.

To achieve greater clarity we first prove this result for reversible CA in the more general class of sofic subshifts. We will appeal to the proof of the following theorem during the course of the proof of our main result.

Theorem 4.2.1. For reversible CA $F : X \to X$ on sofic shifts such that $\lambda^+(F) \in [0, \frac{5}{3}] \cup \{2\}$ it is undecidable whether $\lambda^+(F) \le \frac{5}{3}$ or $\lambda^+(F) = 2$.

Proof. We will reduce the decision problem of Lemma 4.1.7 to the present problem. Let $G : A_2^{\mathbb{Z}} \to A_2^{\mathbb{Z}}$ be a given reversible radius-$\frac{1}{2}$ cellular automaton and $B \subseteq A_2$ some given set. Let $A_1 = \{0, \|, \leftarrow, \rightarrow, \swarrow, \searrow\}$ and define a sofic shift $Y \subseteq A_1^{\mathbb{Z}}$ as the set of those configurations containing a symbol from $Q = \{\leftarrow, \rightarrow, \swarrow, \searrow\}$ in at most one position. We will interpret elements of Q as particles going in different directions at different speeds and which bounce between walls denoted by $\|$. Let $S : Y \to Y$ be the reversible radius-2 CA which does not move occurrences of $\|$ and which moves $\leftarrow$ (resp. $\rightarrow$, $\swarrow$, $\searrow$) to the left at speed 2 (resp. to the right at speed 2, to the left at speed 1, to the right at speed 1) with the additional condition that when an arrow meets a wall, it changes into the arrow with the same speed and opposing direction. More precisely, S is the CA with memory 2 and anticipation 2 determined by the local rule $f : A_1^5 \to A_1$ defined as follows (where $*$ denotes arbitrary symbols):

$$\begin{array}{ll}
f(\rightarrow, 0, 0, *, *) = \rightarrow & f(*, \searrow, 0, *, *) = \searrow \\
f(*, \rightarrow, 0, \|, *) = \leftarrow & f(*, *, \searrow, 0, *) = 0, \\
f(*, *, \rightarrow, 0, *) = 0 & f(*, *, \searrow, \|, *) = \swarrow, \\
f(*, 0, \rightarrow, \|, *) = 0 & \\
f(*, \|, \rightarrow, \|, *) = \rightarrow & \\
f(*, *, 0, \rightarrow, \|) = \leftarrow &
\end{array}$$

with symmetric definitions for arrows in the opposite directions at reflected positions and $f(*, *, a, *, *) = a$ ($a \in A_1$) otherwise. Then let $X = Y \times A_2^{\mathbb{Z}}$ and $\pi_1 : X \to Y$, $\pi_2 : X \to A_2^{\mathbb{Z}}$ be the natural projections $\pi_i(x_1, x_2) = x_i$ for $x_1 \in Y, x_2 \in A_2^{\mathbb{Z}}$ and $i \in \{1, 2\}$.

Let $x_1 \in Y$ and $x_2 \in A_2^{\mathbb{Z}}$ be arbitrary. We define reversible CA $G_2, F_1 : X \to X$ by $G_2(x_1, x_2) = (x_1, G^{10}(x_2))$, $F_1(x_1, x_2) = (S(x_1), x_2)$. Additionally, let $F_2 : X \to X$ be the involution which maps (x_1, x_2) as follows: F_2 replaces an occurrence of $\rightarrow 0 \in A_1^2$ in x_1 at a coordinate $i \in \mathbb{Z}$ by an occurrence of $\swarrow \| \in A_1^2$ (and vice versa) *if and only if*

$$G^j(x_2)[i] \notin B \text{ for some } 0 \le j \le 5$$
$$\text{or } G^j(x_2)[i+1] \notin B \text{ for some } 5 \le j \le 10,$$

and otherwise F_2 makes no changes. Finally, define $F = F_1 \circ G_2 \circ F_2 : X \to X$. The reversible CA F works as follows. Typically particles from Q move in the upper layer in the intuitive manner indicated by the map S and the lower layer is transformed according to the map G^{10}. There are some exceptions to the usual particle movements: If there is a particle $\to$ which does not have a wall immediately at the front and x_2 does not satisfy a local immortality condition in the next 10 time steps, then $\to$ changes into $\swarrow$ and at the same time leaves behind a wall segment $\|$. Conversely, if there is a particle $\swarrow$ to the left of the wall $\|$ and x_2 does not satisfy a local immortality condition, $\swarrow$ changes into $\to$ and removes the wall segment.

We will show that $\lambda^+(F) = 2$ if G is $(1,5)$-locally immortal with respect to B and $\lambda^+(F) \leq \frac{5}{3}$ otherwise. Intuitively the reason for this is that if $x, y \in X$ are two configurations that differ only to the left of the origin, then the difference between $F^i(x)$ and $F^i(y)$ can propagate to the right at speed 2 only via an arrow $\to$ that travels on top of a $(1,5)$-witness. Otherwise, a signal that attempts to travel to the right at speed 2 is interrupted at bounded time intervals and forced to return at a slower speed beyond the origin before being able to continue its journey to the right. We will give more details.

Assume first that G is $(1,5)$-locally immortal with respect to B. Let $x_2 \in A_2^{\mathbb{Z}}$ be a $(1,5)$-witness and define $x_1 \in Y$ by $x_1[0] = \to$ and $x_1[i] = 0$ for $i \neq 0$. Let $x = (0^{\mathbb{Z}}, x_2) \in X$ and $y = (x_1, x_2) \in X$. It follows that $\pi_1(F^i(x))[2i] = 0$ and $\pi_1(F^i(y))[2i] = \to$ for every $i \in \mathbb{N}$, so $\lambda^+(F) \geq 2$. On the other hand, F has memory 2 so necessarily $\lambda^+(F) = 2$.

Assume then that there are no $(1,5)$-witnesses for G. Let us denote

$$C(n) = \{x \in A_1^{\mathbb{Z}} \mid G^{5i+j}(x)[i] \in B \text{ for } 0 \leq i \leq n, 0 \leq j \leq 5\} \text{ for } n \in \mathbb{N}.$$

Since there are no $(1,5)$-witnesses, by a compactness argument we may fix some $N \in \mathbb{N}_+$ such that $C(2N) = \emptyset$. We claim that $\lambda^+(F) \leq \frac{5}{3}$, so let us assume that $(x^{(n)})_{n\in\mathbb{N}}$ with $x^{(n)} = (x_1^{(n)}, x_2^{(n)}) \in X$ is a sequence of configurations such that $\Lambda_n^+(x^{(n)}, F) = s_n n$ where $(s_n)_{n\in\mathbb{N}}$ tends to λ^+. There exist $y^{(n)} = (y_1^{(n)}, y_2^{(n)}) \in X$ such that $x^{(n)}[i] = y^{(n)}[i]$ for $i > -s_n n$ and $F^{t_n}(x)[i_n] \neq F^{t_n}(y)[i_n]$ for some $0 \leq t_n \leq n$ and $i_n \geq 0$.

First assume that there are arbitrarily large $n \in \mathbb{N}$ for which $x_1^{(n)}[i] \in \{0, \|\}$ for $i > -s_n n$ and consider the subsequence of such configurations $x^{(n)}$ (starting with sufficiently large n). Since G is a one-sided CA, it follows that $\pi_2(F^{t_n}(x^{(n)}))[j] = \pi_2(F^{t_n}(y^{(n)}))[j]$ for $j \geq 0$. Therefore the difference between $x^{(n)}$ and $y^{(n)}$ can propagate to the right only via an arrow from Q, so without loss of generality (by swapping $x^{(n)}$ and $y^{(n)}$ if necessary) $\pi_1(F^{t_n}(x^{(n)}))[j_n] \in Q$ for some $0 \leq t_n \leq n$ and $j_n \geq i_n - 1$. Fix some such t_n, j_n and let $w_n \in Q^{t_n+1}$ be such that $w_n(i)$ is the unique state from Q in the configuration $F^i(x^{(n)})$ for $0 \leq i \leq t_n$. The word w_n has a factorization of the form $w_n = u(v_1 u_1 \cdots v_k u_k)v$ ($k \in \mathbb{N}$) where $v_i \in \{\rightarrow\}^+$, $v \in \{\rightarrow\}^*$ and $u_i \in (Q \setminus \{\rightarrow\})^+$, $u \in (Q \setminus \{\rightarrow\})^*$. By the choice of N it follows that all v_i, v have length at most N and by the definition of the CA F it is easy to see that each u_i contains at least $2(|v_i| - 1) + 1$ occurrences of $\swarrow$ and at least $2(|v_i| - 1) + 1$ occurrences of $\searrow$ (after $\rightarrow$ turns into $\swarrow$, it must return to the nearest wall to the left and back and at least once more turn into $\swarrow$ before turning back into $\rightarrow$. If $\rightarrow$ were to turn into $\leftarrow$ instead, it would signify an impassable wall on the right). If we denote by x_n the number of occurrences of $\rightarrow$ in w_n, then $x_n \leq |w_n|/3 + \mathcal{O}(1)$ (this upper bound is achieved by assuming that $|v_i| = 1$ for every i) and

$$s_n n \leq |w_n| + 2x_n \leq |w_n| + \frac{2}{3}|w_n| + \mathcal{O}(1) \leq \frac{5}{3}n + \mathcal{O}(1).$$

After dividing this inequality by n and passing to the limit we find that $\lambda^+ \leq \frac{5}{3}$.[2]

Next assume that there are arbitrarily large $n \in \mathbb{N}$ for which $x_1^{(n)}[i] \in Q$ for some $i > -s_n n$. The difference between $x^{(n)}$ and $y^{(n)}$ can propagate to the right only after the element from Q in $x^{(n)}$ reaches the coordinate $-s_n n$, so without loss of generality there are $0 < t_{n,1} < t_{n,2} \leq n$ and $i_n \geq 0$ such that $\pi_1(F^{t_{n,1}}(x^{(n)}))[-s] \in Q$ for some $s \geq s_n n$ and $\pi_1(F^{t_{n,2}}(x^{(n)}))[i_n] \in Q$. From this the contradiction follows in the same way as in the previous paragraph. $\square$

We are ready to prove the result for CA on full shifts.

Theorem 4.2.2. For reversible CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ such that $\lambda^+(F) \in [0, \frac{5}{3}] \cup \{2\}$ it is undecidable whether $\lambda^+(F) \leq \frac{5}{3}$ or $\lambda^+(F) = 2$.

Proof. Let $G : A_2^{\mathbb{Z}} \to A_2^{\mathbb{Z}}$, A_1, $F = F_1 \circ G_2 \circ F_2 : X \to X$, etc. be as in the proof of the previous theorem. We will adapt the conveyor belt construction from [21] to define a CA F' on a full shift which simulates F and has the same right Lyapunov exponent as F.

Denote $Q = \{\leftarrow, \rightarrow, \swarrow, \searrow\}$, $\Sigma = \{0, \|\}$, $\Delta = \{-, 0, +\}$, define the alphabets

$$\Gamma = (\Sigma^2 \times \{+, -\}) \cup (Q \times \Sigma \times \{0\}) \cup (\Sigma \times Q \times \{0\}) \subseteq A_1 \times A_1 \times \Delta$$

and $A = \Gamma \times A_2$ and let $\pi_{1,1}, \pi_{1,2} : A^{\mathbb{Z}} \to A_1^{\mathbb{Z}}$, $\pi_\Delta : A^{\mathbb{Z}} \to \Delta^{\mathbb{Z}}$, $\pi_2 : A^{\mathbb{Z}} \to A_2^{\mathbb{Z}}$ be the natural projections $\pi_{1,1}(x) = x_{1,1}$, $\pi_{1,2}(x) = x_{1,2}$, $\pi_\Delta(x) = x_\Delta$, $\pi_2(x) = x_2$ for $x = (x_{1,1}, x_{1,2}, x_\Delta, x_2) \in A^{\mathbb{Z}} \subseteq (A_1 \times A_1 \times \Delta \times A_2)^{\mathbb{Z}}$. For arbitrary $x = (x_1, x_2) \in (\Gamma \times A_2)^{\mathbb{Z}}$ define $G_2' : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $G_2'(x) = (x_1, G^{10}(x_2))$.

[2] By performing more careful estimates it can be shown that $\lambda^+ = 1$, but we will not attempt to formalize the argument for this.

Next we define $F_1' : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$. Every element $x = (x_1, x_2) \in (\Gamma \times A_2)^{\mathbb{Z}}$ has a unique decomposition of the form

$$(x_1, x_2) = \cdots (w_{-2}, v_{-2})(w_{-1}, v_{-1})(w_0, v_0)(w_1, v_1)(w_2, v_2) \cdots$$

where

$$\begin{aligned} w_i \in &(\Sigma^2 \times \{+\})^*((Q \times \Sigma \times \{0\}) \cup (\Sigma \times Q \times \{0\}))(\Sigma^2 \times \{-\})^* \\ &\cup (\Sigma^2 \times \{+\})^*(\Sigma^2 \times \{-\})^* \end{aligned}$$

with the possible exception of the leftmost w_i beginning or the rightmost w_i ending with an infinite sequence from $\Sigma^2 \times \{+, -\}$.

Let $(c_i, e_i) \in (\Sigma \times \Sigma)^*((Q \times \Sigma) \cup (\Sigma \times Q))(\Sigma \times \Sigma)^* \cup (\Sigma \times \Sigma)^*$ be the word that is derived from w_i by removing the symbols from Δ. The pair (c_i, e_i) can be seen as a conveyor belt by gluing the beginning of c_i to the beginning of e_i and the end of c_i to the end of e_i. The map F_1' will shift arrows like the map F_1, and at the junction points of c_i and e_i the arrow can turn around to the opposite side of the belt. More precisely, define the permutation $\rho : A_1 \to A_1$ by

$$\begin{array}{llll} \rho(0) = 0 & \rho(\|) = \| & & \\ \rho(\leftarrow) = \rightarrow & \rho(\rightarrow) = \leftarrow & \rho(\swarrow) = \searrow & \rho(\searrow) = \swarrow \end{array}$$

and for a word $u \in A_1^*$ let $\rho(u)$ denote the coordinatewise application of ρ. For any word $w = w[1] \cdots w[n]$ define its reversal by $w^R[i] = w[n + 1 - i]$ for $1 \leq i \leq n$. Then consider the periodic configuration $y = [(c_i, v_i)(\rho(e_i), v_i)^R]^{\mathbb{Z}} \in (A_1 \times A_2)^{\mathbb{Z}}$. The map $F_1 : X \to X$ extends naturally to configurations of the form y: y can contain infinitely many arrows, but they all point in the same direction and occur in identical contexts. By applying F_1 to y we get a new configuration of the form $[(c_i', v_i)(\rho(e_i'), v_i)^R]$. From this we extract the pair (c_i', e_i'), and by adding plusses and minuses to the left and right of the arrow (or in the same coordinates as in (c_i, e_i) if there is no occurrence of an arrow) we get a word w_i' which is of the same form as w_i. We define $F_1' : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $F_1'(x) = x'$ where $x' = \cdots (w_{-2}', v_{-2})(w_{-1}', v_{-1})(w_0', v_0)(w_1', v_1)(w_2', v_2) \cdots$. Clearly F_1' is shift invariant, continuous and reversible.

We define the involution $F_2' : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ as follows. For $x \in A^{\mathbb{Z}}$ and $j \in \{1, 2\}$ F_2' replaces an occurrence of $\rightarrow 0$ in $\pi_{1,j}(x)$ at coordinate $i \in \mathbb{Z}$ by an occurrence of $\swarrow \|$ (and vice versa) *if and only if* $\pi_\Delta(x)[i+1] = -$ and

$$\begin{aligned} &G^j(\pi_2(x))[i] \notin B \text{ for some } 0 \leq j \leq 5 \\ \text{or } &G^j(\pi_2(x))[i+1] \notin B \text{ for some } 5 \leq j \leq 10, \end{aligned}$$

and otherwise F_2 makes no changes. F_2' simulates the map F_2 and we check the condition $\pi_\Delta(x)[i+1] = -$ to ensure that F_2' does not transfer information between neighboring conveyor belts.

Finally, we define $F' = F_1' \circ G_2' \circ F_2' : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$. The reversible CA F' simulates $F : X \to X$ simultaneously on two layers and it has the same right Lyapunov exponent as F. $\square$

The following corollary is immediate.

Corollary 4.2.3. There is no algorithm that, given a reversible CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ and a rational number $\epsilon > 0$, returns the Lyapunov exponent $\lambda^+(F)$ within precision ϵ.

Note that this result does not restrict the size of the alphabet A of the CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ whose Lyapunov exponents are to be determined. Standard encoding methods might be sufficient to solve the following problem.

Problem 4.2.4. Is there a fixed mixing SFT X such that the Lyapunov exponents of a given reversible CA $F : X \to X$ cannot be computed to arbitrary precision? Can we choose here $X = \Sigma_2^{\mathbb{Z}}$? Can X be any mixing SFT?

In our constructions we controlled only the right exponent λ^+ and let the left exponent λ^- vary freely. Controlling both Lyapunov exponents would be necessary to answer the following.

Problem 4.2.5. Is it decidable whether the equality $\lambda^+(F) + \lambda^-(F) = 0$ holds for a given reversible cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$?

We mentioned at the beginning of this chapter that there exists a single CA whose topological entropy is an uncomputable number. We ask whether a similar result holds also for the Lyapunov exponents.

Problem 4.2.6. Does there exist a single cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ such that $\lambda^+(F)$ is an uncomputable number?

By an application of Fekete's lemma the limit that defines $\lambda^+(F)$ is actually the infimum of a sequence whose elements are easily computable when $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a CA on a full shift. This yields the natural obstruction that $\lambda^+(F)$ has to be an upper semicomputable number. We are not aware of a cellular automaton on a full shift that has an irrational Lyapunov exponent (see Question 5.7 in [12]), so constructing such a CA (or proving the impossibility of such a construction) should be the first step. This problem has an answer for CA $F : X \to X$ on general subshifts X, and furthermore for every real $t \geq 0$ there is a subshift X_t and a reversible CA $F_t : X_t \to X_t$ such that $\lambda^+(F_t) = \lambda^-(F_t) = t$ [25]. Also recall that by Theorem 3.7.2 there are reversible CA $\Pi_{p,pq}$ with irrational *average* Lyapunov exponents (with respect to the uniform measure).

Chapter 5

Glider Automata

We saw in Section 3.2 that the multiplication automata $\Pi_{p,n}$ are partitioned automata whenever p is a factor of n. This automaton is equal to Id or σ if $p = 1$ or $p = n$ respectively, so interesting dynamics can only occur if $1 < p < n$, and then the definition of $\Pi_{p,n}$ involves a nontrivial partial shift map $\tau_p : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$. A typical space-time diagram of a canonical partial shift $\tau_p : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ for $p = 2$, $n = 4$ with respect to a finite point x can be seen in Figure 5.1.

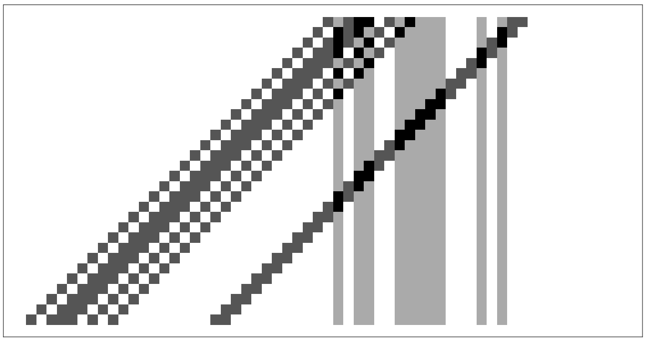

Figure 5.1: The space-time diagram of $x \in \Sigma_4$ under the canonical partial shift τ_2. Squares ranging from white to black correspond to digits from 0 to 3.

Not all subshifts can be decomposed into a cartesian product of two nontrivial subshifts (in particular this cannot be done for full shifts with an alphabet of prime cardinality), so a possible first step to constructing dynamically complex cellular automata on more general subshifts X would be to construct sensible analogues of partial shift maps on X. We will define a class of reversible CA we call *diffusive glider CA* and we prove that they exist on all mixing sofic shifts (and in particular on all full shifts). They will be similar to partial shifts in the sense that they can be used to decompose any finite configuration into two distinct collections of “gliders” that can travel throughout the configuration similarly as in Figure 5.1.

The existence of analogues of such diffusive glider CA G on more general subshifts X is interesting also because G can be used to convert an arbitrary finite $x \in X$ into another configuration $G^t(x)$ (for some $t \in \mathbb{N}_+$) with a simpler structure, which nevertheless contains all the information concerning the original point x because G is invertible. Such maps have been successfully applied to other problems. We give some examples. The paper [53] contains a construction of a finitely generated group $\mathcal{G} \subseteq \mathrm{Aut}(\Sigma_4^{\mathbb{Z}})$ whose elements can implement any permutation on any finite collection of 0-finite non-constant configurations that belong to different shift orbits. An essential part of the construction is that one of the generators of $\mathcal{G}$ is a partial shift on $\Sigma_4^{\mathbb{Z}}$. Another example is the construction of a physically universal cellular automaton G on $\Sigma_{16}^{\mathbb{Z}}$ in [54]. Also here it is essential that G is a diffusive glider CA (but G also implements certain additional collision rules for gliders).

5.1 First Constructions: the Case of Full Shifts

Before proceeding in the full generality of mixing sofic shifts we first present simpler constructions of diffusive glider CA on full shifts. We will also postpone the precise definition of a diffusive glider CA until Section 5.3.

5.1.1 Full Shifts $\Sigma_n^{\mathbb{Z}}$ with $n > 2$

In this subsection we cover the case of the full shift $\Sigma_n^{\mathbb{Z}}$ for $n \geq 3$. Fix some such n for the rest of the subsection and denote $s = n - 1$.

Define permutations $\pi_-, \pi_+ : \Sigma_n \to \Sigma_n$ by

$$\pi_-(i) = \begin{cases} s \text{ when } i = s, \\ s-1 \text{ when } i = 0, \\ i-1 \text{ otherwise,} \end{cases} \qquad \pi_+(i) = \begin{cases} 0 \text{ when } i = 0, \\ 1 \text{ when } i = s, \\ i+1 \text{ otherwise.} \end{cases}$$

Using these permutations we define cellular automata $P_-, P_+ : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ by $P_+(x)[i] = \pi_+(x[i])$ and

$$P_-(x)[i] = \begin{cases} \pi_-(x[i]) \text{ when } x[i-1] = s \text{ or } x[i+1] = s, \\ x[i] \text{ otherwise.} \end{cases}$$

Finally, let $G_n = P_+ \circ P_-$. We may drop the subscript n when the size of the alphabet is clear from the context. This is a radius-1 reversible CA and it can be defined by a local rule which is symmetric with respect to the origin.

The space-time diagram of a typical finite configuration $x \in \Sigma_3^{\mathbb{Z}}$ with respect to G_3 is plotted in Figure 5.2. It can be seen that x eventually diffuses into two different "fleets" traveling in two opposing directions. In Theorem 5.1.2 we will prove that this diffusion happens eventually no matter which finite initial configuration is chosen.

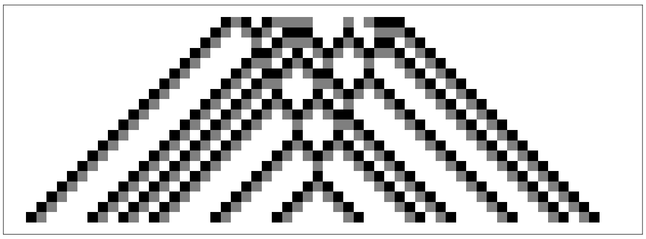

Figure 5.2: The diffusion of $x \in \Sigma_3^{\mathbb{Z}}$ under the map $G_3 : \Sigma_3^{\mathbb{Z}} \to \Sigma_3^{\mathbb{Z}}$. White, gray and black squares correspond to digits 0, 1 and 2 respectively.

The CA G admits a leftward traveling glider $\boxed{\leftarrow} = s1$ in the sense that if $x \in \Sigma_n^{\mathbb{Z}}$ contains the pattern $0s1$ at some position, then $G(x)$ contains the pattern $s10$ at the same position. Similarly there is a rightward traveling glider $\boxed{\rightarrow} = 1s$ ($1s0$ changes into $01s$). We call elements of the sets

$$\mathrm{GF}_\ell = {}^\infty 0(\boxed{\leftarrow}00^*)^*0^\infty, \qquad \mathrm{GF}_r = {}^\infty 0(0^*0\boxed{\rightarrow})^*0^\infty$$

left and right glider fleets (note that these are finite configurations). Elements of $\mathrm{GF} = \mathrm{GF}_\ell \cup \mathrm{GF}_r$ are called glider fleets. The sets GF_ℓ and GF_r are invariant under the map G.

Assuming that $x \notin \mathrm{GF}_\ell$ is a non-zero finite configuration, it has a unique decomposition of the form

$$x = {}^\infty 0\boxed{\leftarrow}00^*\boxed{\leftarrow}00^* \cdots \boxed{\leftarrow}00^* x[i,\infty],$$

where $i \in \mathbb{Z}$ is such that $x[i] \neq 0$ and $x[i, i+2] \neq \boxed{\leftarrow}0$, in which case we say that the *left bound* of x is i. Similarly, if $x \notin \mathrm{GF}_r$ is a non-zero finite configuration, it has a unique decomposition of the form

$$x = x[-\infty, i]0^*0\boxed{\rightarrow} \cdots 0^*0\boxed{\rightarrow}0^*0\boxed{\rightarrow}0^\infty,$$

where $i \in \mathbb{Z}$ is such that $x[i] \neq 0$ and $x[i-2, i] \neq 0\boxed{\rightarrow}$, in which case we say that the *right bound* of x is i.

Lemma 5.1.1. Assume that $x \neq 0^{\mathbb{Z}}$ is a finite configuration with left bound i (resp. right bound i). Then there exists $t \in \mathbb{N}_+$ such that the left bound (resp. right bound) of $G^t(c)$ is strictly greater (resp. smaller) than i. Moreover, the left bound (resp. the right bound) of $G^{t'}(x)$ is at least $i-1$ (resp. at most $i+1$) for all $t' \in \mathbb{N}$.

Proof. Since the local rule of G is symmetric, it suffices to consider the case where x has left bound i. Note that the gliders to the left of the coordinate i move to the left at constant speed under action of G without being affected by the remaining part of the configuration. Without loss of generality we may assume that $x[i] = s$ or $x[i+1] = s$: otherwise we consider instead the configuration $G^t(x)$, where $t \in \mathbb{N}$ is the smallest integer such that $G^t(x)[i] = s$ or $G^t(x)[i+1] = s$ (note that the left bound of $G^t(x)$ is at least i, and if it strictly greater than i, we have reached the conclusion of the lemma).

Assume first that $x[i] = s$. Then $G(x)[i-2, i] = 0s1$ and $G^2(x)[i-3, i] = 0s10 = 0\boxed{\leftarrow}0$, so the left bound of $G^2(x)$ is at least $i+1$.

Assume then that $x[i, i+1] = cs$, where $1 < c < s$. Then $G(x)[i, i+1] = c1$ and we may choose the smallest $t \in \mathbb{N}_+$ such that either $G^t(G(x))[i] = s$, in which case we reach the conclusion by arguing as in the previous paragraph, or $G^t(G(x))[i, i+1] = ds$ where $c < d < s$, in which case we may repeat inductively the argument in this paragraph.

Assume finally that $x[i, i+1] = 1s$. Then $G(x)[i, i+1] = 01$ and the left bound of $G(x)$ is at least $i+1$. $\square$

Using this lemma we get the following theorem.

Theorem 5.1.2. If $x \in \Sigma_n^{\mathbb{Z}}$ is a finite configuration, then for every $N \in \mathbb{N}$ there exists $t \in \mathbb{N}$ such that $G^t(x)[-N, N] = 0^{2N+1}$, $G^t(x)$ contains only $\boxed{\leftarrow}$-gliders (separated by some zeroes) to the left of coordinate $-N$ and only $\boxed{\rightarrow}$-gliders (separated by some zeroes) to the right of coordinate N.

Proof. Clearly the claim holds if $x \in \mathrm{GF}$. Otherwise we may apply the previous lemma inductively to get $t_\ell, t_r \in \mathbb{N}$ such that $G^{t_\ell}(x)$ has left bound at least $N+2$ and $G^{t_r}(x)$ has right bound at most $-(N+2)$. Let $t = \max\{t_\ell, t_r\}$: then $G^t(x)$ has left bound at least $N+1$ and right bound at most $-(N+1)$, proving the theorem. $\square$

5.1.2 The Full Shift $\Sigma_2^{\mathbb{Z}}$

The construction of diffusive glider CA presented in the previous subsection does not directly generalize to the binary full shift. We will use a slightly different approach to construct such automata on $\Sigma_2^{\mathbb{Z}}$. In the next subsection we will see that some modifications to this approach allows us to construct diffusive glider CA on all nontrivial mixing sofic shifts.

First we define involutive cellular automata $P_1, P_2 : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$ as follows. In any $x \in \Sigma_2^{\mathbb{Z}}$,

- P_1 replaces every occurrence of 0010 by 0110 and vice versa
- P_2 replaces every occurrence of 0100 by 0110 and vice versa.

See Figure 5.3 for a space-time diagram of a typical finite point with respect to $G' = P_2 \circ P_1$. In this figure we see that G' admits gliders (finite patterns that travel through the configuration) but also large blocks of ones which do not diffuse under the action of G'. In particular, G' cannot ever change any occurrence of the word 111 in any configuration, because P_1 only flips occurrences of 0010 and 0110 and P_2 only flips occurrences of 0100 and 0110.

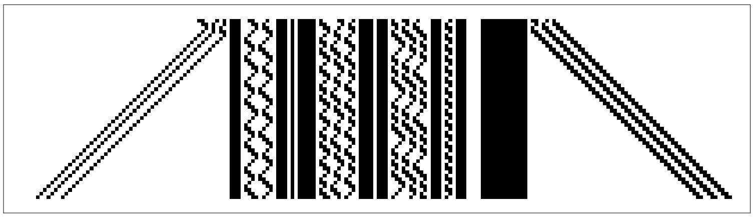

Figure 5.3: Action of $G' : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$ on a typical finite configuration. White and black squares correspond to digits 0 and 1 respectively.

To dissolve large blocks of ones we define one more involutive CA $P_3 : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$ such that in any $x \in \Sigma_2^{\mathbb{Z}}$,

- P_3 replaces every occurrence of 00111 by 00101 and vice versa.

Finally we may define $G = P_3 \circ G' = P_3 \circ P_2 \circ P_1$. See Figure 5.4 for a space-time diagram of a typical finite point with respect to G. Similarly as in Figure 5.2 we see that x eventually diffuses into two distinct components that travel in two opposing directions. In Theorem 5.1.5 we will prove that this diffusion happens eventually no matter which finite initial configuration is chosen.

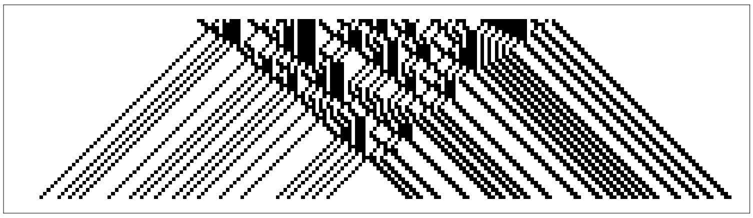

Figure 5.4: The diffusion of $x \in \Sigma_2^{\mathbb{Z}}$ under the map $G : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$. White and black squares correspond to digits 0 and 1 respectively.

Define a leftbound glider $\boxed{\leftarrow} = 01$ and a rightbound glider $\boxed{\rightarrow} = 11$. We call elements of the sets

$$\mathrm{GF}_{\ell} = {}^{\infty}0(\boxed{\leftarrow}00^*)^*0^{\infty}, \qquad \mathrm{GF}_{\reflectbox{ℓ}} = {}^{\infty}0(0^*0\boxed{\rightarrow})^*0^{\infty}$$

left and right glider fleets (note that these are finite configurations). Elements of $\mathrm{GF} = \mathrm{GF}_{\ell} \cup \mathrm{GF}_{\reflectbox{ℓ}}$ are called glider fleets. These names are justified since $G(x) = \sigma(x)$ for $x \in \mathrm{GF}_\ell$ and $G(x) = \sigma^{-1}(x)$ for $x \in \mathrm{GF}_r$ (and this would hold even if G were to be replaced by G'). As we will see, the role of the map P_3 is, for a given finite configuration x, to “erode” non-zero non-glider parts of x from the left and to turn the eroded parts into new gliders. Assuming that $x \notin \mathrm{GF}_\ell$ is a non-zero finite configuration, it has a unique decomposition of the form

$$x = {}^\infty 0(100)0^*(100)0^* \cdots (100)0^* x[i, \infty],$$

where $i \in \mathbb{Z}$ is such that $x[i] = 1$ and $x[i, i+2] \neq 100$, in which case we say that the *left bound* of x is i. Similarly, if $x \notin \mathrm{GF}_r$ is a non-zero finite configuration, it has a unique decomposition of the form

$$x = x[-\infty, i]0^*(011) \cdots 0^*(011)0^*(011)0^\infty,$$

where $i \in \mathbb{Z}$ is such that $x[i] = 1$ and $x[i-2, i] \neq 011$, in which case we say that the *right bound* of x is i.

Lemma 5.1.3. Assume that $x \neq 0^{\mathbb{Z}}$ is a finite configuration with left bound i. Then there exists $t \in \mathbb{N}_+$ such that the left bound of $G^t(x)$ is strictly greater than i. Moreover, the left bound of $G^{t'}(x)$ is at least i for all $t' \in \mathbb{N}$.

Proof. Note that the gliders to the left of the coordinate i move to the left at constant speed under action of G without being affected by the remaining part of the configuration. Since the left bound of x is i, we must have $x[i-2, i+2] \in \{00110, 00101, 00111\}$.

Assume first that $x[i-2, i+2] = 00110$. Then $P_1(x)[i-2, i+2] = 00010$, $P_2(P_1(x))[i-2, i+1] = 0001$ and $G(x)[i-2, i+1] = 0001$, so the left bound of $G(x)$ is at least $i+1$.

Assume then that $x[i-2, i+2] = 00101$. Then $P_1(x)[i-2, i+1] = 0110$, $P_2(P_1(x))[i-3, i+1] = 00100$ and $G(x)[i-3, i+1] = 00100$, so the left bound of $G(x)$ is at least $i+2$.

Assume finally that $x[i-2, i+2] = 00111$. Then $P_2(P_1(x))[i-2, i+2] = 00111$ and $G(x)[i-2, i+2] = 00101$. By the previous case it follows that $G^2(x)[i-3, i+1] = 00100$, so the left bound of $G^2(x)$ is at least $i+2$. $\square$

Lemma 5.1.4. Assume that $x \neq 0^{\mathbb{Z}}$ is a finite configuration with right bound i. Then there exists $t \in \mathbb{N}_+$ such that the right bound of $G^t(x)$ is strictly less than i. Moreover, the right bound of $G^{t'}(x)$ is at most $i+1$ for all $t' \in \mathbb{N}$.

Proof. Note that the gliders to the right of the coordinate i move to the right at constant speed under action of G without being affected by the remaining part of the configuration. Since the right bound of x is i, we must have $x[i-2, i+1] \in \{0010, 1110, 1010\}$.

Assume first that $x[i-2, i+1] = 0010$. Then $P_1(x)[i-2, i+1] = 0110$, $P_2(P_1(x))[i-2, i+1] = 0100$ and $G(x)[i-1, i+1] = 100$, so the right bound of $G(x)$ is at most $i-1$.

Assume then that $x[i-2, i+1] = 1110$. By repeated application of the previous lemma there exists $t' \in \mathbb{N}_+$ such that the left bound of $G^{t'}(x)$ is at least i, so in particular $G^{t'}(x)[i-2, i+1] \neq 1110$. Let $t \in \mathbb{N}_+$ be the minimal number such that $G^t(x)[i-2, i+1] \neq 1110$. This is possible only if $P_2(P_1(G^{t-1}(x)))[i-4, i+1] = 001110$, so $G^t(x)[i-4, i+1] = 001010$. Then $P_1(G^t(x))[i-4, i+2] = 0110100$, $P_2(P_1(G^t(x)))[i-4, i+2] = 0100110$ and $G^{t+1}(x)[i-3, i+2] = 100110$, so the right bound of $G^{t+1}(x)$ is at most $i-3$.

Assume finally that $x[i-2, i+1] = 1010$. Then $P_1(x)[i-2, i+2] = 10100$, $P_2(P_1(x))[i-1, i+2] = 0110$ and $G(x)[i-1, i+2] \in \{0110, 1110\}$. If $G(x)[i-1, i+2] = 0110$, then the right bound of $G(x)$ is at most $i-2$. Otherwise, if $G(x)[i-1, i+2] = 1110$, the right bound of $G(x)$ is equal to $i+1$. Then by the previous case there is $t \in \mathbb{N}_+$ such that $G^{t+1}(G(x))[i-2, i+3] = 100110$, so the right bound of $G^{t+2}(x)$ is at most $i-2$. $\square$

Using these lemmas we get the following theorem.

Theorem 5.1.5. If $x \in \Sigma_2^{\mathbb{Z}}$ is a finite configuration, then for every $N \in \mathbb{N}$ there exists $t \in \mathbb{N}$ such that $G^t(x)[-N, N] = 0^{2N+1}$, $G^t(x)$ contains only $\boxed{\leftarrow}$-gliders (separated by some zeroes) to the left of coordinate $-N$ and only $\boxed{\rightarrow}$-gliders (separated by some zeroes) to the right of coordinate N.

Proof. Clearly the claim holds if $x \in \mathrm{GF}$. Otherwise we may apply the previous lemmas inductively to get $t_\ell, t_r \in \mathbb{N}$ such that $G^{t_\ell}(x)$ has left bound at least $N+2$ and $G^{t_r}(x)$ has right bound at most $-(N+2)$. Let $t = \max\{t_\ell, t_r\}$: then $G^t(x)$ has left bound at least $N+2$ and right bound at most $-(N+1)$, proving the theorem. $\square$

5.2 Mixing Sofic Shifts

In this section we construct for an arbitrary nontrivial mixing sofic shift X (with a distinguished periodic point $\mathbf{0}^{\mathbb{Z}}$) a reversible CA G_X which breaks every $\mathbf{0}$-finite point of X into a collection of gliders traveling in opposite directions. Almost all parts of this construction will be done in the more general class of synchronizing subshifts for two reasons. The first one is that the statements and proofs of the auxiliary lemmas become simpler without using the extra structure of soficness. The second reason is that we will later give examples of subshifts with specification (which are in particular synchronizing) on which no analogue of this construction can work. In light of this it will be instructive to pinpoint the precise part of the construction that requires the assumption of soficness.

Definition 5.2.1. Given a subshift X, we say that a word $w \in L(X)$ is (intrinsically) synchronizing if

$$\forall u, v \in L(X) : uw, wv \in L(X) \implies uwv \in L(X).$$

We say that a transitive subshift X is synchronizing if $L(X)$ contains a synchronizing word.

Transitive sofic shifts in particular are synchronizing, which follows by using the results of [43] in Section 3.3 and in Exercise 3.3.3.

Definition 5.2.2. Let X be any subshift. The set of contexts of $w \in L(X)$ is defined by $\mathrm{C}_X(w) = \{(w_1, w_2) \mid w_1 w w_2 \in L(X)\}$. We define an equivalence relation called the *syntactic relation* on $L(X)$ as follows. For any $u, v \in L(X)$ let $u \sim v$ if $\mathrm{C}_X(u) = \mathrm{C}_X(v)$. The equivalence class containing $w \in L(X)$ is denoted by $\mathrm{S}_X(w)$ and the collection of all equivalence classes is denoted by S_X. The subscript X can be omitted when the subshift is clear from the context. By adjoining a zero element 0 to S_X we get a *syntactic monoid* where multiplication is defined by $S_X(u)S_X(v) = S_X(uv)$ if $uv \in L(X)$, and otherwise the product of two elements is equal to 0. It is easy to show that this monoid operation is well defined.

Lemma 5.2.3. Let X be a subshift and $u, v \in L(X)$ synchronizing words. If $w_1, w_2 \in L(X)$ are words both of which have u as a prefix and v as a suffix, then $S_X(w_1) = S_X(w_2)$.

Proof. Let $t_1, t_2 \in L(X)$ be such that $t_1 w_1 t_2 \in L(X)$. In particular $t_1 u \in L(X)$ and by assumption $w_2 \in L(X)$, so by using the fact that u is synchronizing it follows that $t_1 w_2 \in L(X)$. We also know that $v t_2 \in L(X)$, so by using the fact that v is synchronizing it follows that $t_1 w_2 t_2 \in L(X)$. By symmetry, from $t_1 w_2 t_2 \in L(X)$ it would follow that $t_1 w_1 t_2 \in L(X)$, which proves the lemma. □

It is known that a subshift X is sofic if and only if S_X is finite, see e.g. Theorem 6.1.2 in [36].

Definition 5.2.4. Given a subshift $X \subseteq A^{\mathbb{Z}}$, we say that $w \in L(X)$ has a unique successor in X (resp. a unique predecessor) if $wa \in L(X)$ (resp. $aw \in L(X)$) for a unique $a \in A$. Then we say that a is the unique successor (resp. the unique predecessor) of w.

Definition 5.2.5. Let $X \subseteq A^{\mathbb{Z}}$ be a subshift and let $w = w_1 \cdots w_n \in L(X)$ with all $w_i \in A$ distinct. If w_i have unique successors for $1 \leq i < n$, we say that w is future deterministic in X and if w_j have unique predecessors for $1 < j \leq n$, we say that w is past deterministic in X. If w is both future and past deterministic in X, we say that w is deterministic in X.

Lemma 5.2.6. Let $X \subseteq A^{\mathbb{Z}}$ be a subshift and let $A' = \{a' \mid a \in A\}$. If $\psi : X \to X' \subseteq (A \cup A')^{\mathbb{Z}}$ is a surjective morphism and for all $x \in X$, $i \in \mathbb{Z}$, $a \in A$ it holds that $\psi(x)[i] \in \{a, a'\} \implies x[i] = a$ (i.e. ψ does nothing else in configurations than add some primes as superscripts), then ψ is a conjugacy. Furthermore, let $w = w_1 \cdots w_n \in L(X) \cap L(X')$ and $w' = w_1' \cdots w_n'$. Then also the following hold.

- Assume that $w_i w_{i+1}', w_i' w_{i+1} \notin L(X')$ for $1 \leq i < n$. If w is future (resp. past) deterministic in X, then w is future (resp. past) deterministic also in X'.

- Assume that w is a synchronizing word for X which is blocking with respect to ψ in the sense that for all $x, y \in X$ satisfying $\psi(x)[0, n-1] = \psi(y)[0, n-1] = w$,

  $$x[0, \infty] = y[0, \infty] \implies \psi(x)[0, \infty] = \psi(y)[0, \infty] \text{ and}$$
  $$x[-\infty, n-1] = y[-\infty, n-1] \implies \psi(x)[-\infty, n-1] = \psi(y)[-\infty, n-1].$$

  Then w is a synchronizing word for X'.

Proof. To see that ψ is a conjugacy it suffices to show that ψ is injective, but this is obvious.

Now assume that w satisfies the assumption in the first item and that w is future deterministic in X. We show that w is future deterministic in X'. To see that w_i $(1 \leq i < n)$ has a unique successor in X', let $x \in X$ be such that $\psi(x)[0] = w_i$. Then also $x[0] = w_i$ and since w is future deterministic in X it follows that $x[0, 1] = w_i w_{i+1}$ and $\psi(x)[0, 1] \in \{w_i w_{i+1}, w_i w_{i+1}'\}$. Since by assumption $w_i w_{i+1}' \notin L(X')$, it follows that $\psi(x)[0, 1] = w_i w_{i+1}$ and w_{i+1} is the unique successor of w_i in X'. The proof for past determinism is symmetric.

Now assume that w satisfies the assumption in the second item. Assume that $x_1', x_2' \in X'$ both have an occurrence of w at the origin. To see that w is a synchronizing word of X', we need to show that $x_1' \otimes x_2'$ (the gluing of x_1' and x_2' at the origin) belongs to X'. Let therefore $x_1, x_2 \in X$ be such that $\psi(x_i) = x_i'$, so in particular both x_i have an occurrence of w at the origin. Since w is synchronizing in X it follows that $x_1 \otimes x_2 \in X$. From the blocking property of w it follows that $x_1' \otimes x_2' = \psi(x_1) \otimes \psi(x_2) = \psi(x_1 \otimes x_2) \in X'$. $\square$

Lemma 5.2.7. Let $X \subseteq A^{\mathbb{Z}}$ be a subshift and let $A' = \{a' \mid a \in A\}$. Given $w = w_1 \cdots w_n \in L(X)$ with all $w_i \in A$ distinct there is a conjugacy $\psi : X \to X' \subseteq (A \cup A')^{\mathbb{Z}}$ such that $w \in L(X')$ and w is future deterministic in X'. Moreover, if $w^{\mathbb{Z}} \in X$ then $w^{\mathbb{Z}} \in X'$, and if w is a synchronizing word of X then w is a synchronizing word of X'.

Proof. Let $\psi : X \to (A \cup A')^{\mathbb{Z}}$ be a morphism defined by

$$\psi(x)[i] = \begin{cases} x[i]' & \text{when } x[i] = w_j \text{ and } x[i, i+n-j] \neq w_j w_{j+1} \cdots w_n \\ & \text{for some } 1 \leq j < n, \\ x[i] & \text{otherwise.} \end{cases}$$

By Lemma 5.2.6 ψ induces a conjugacy between X and $X' = \psi(X)$. If $x \in X$ contains an occurrence of w at the origin, then $\psi(x)$ also contains an occurrence of w at the origin and $w \in L(X')$. If $w^{\mathbb{Z}} \in X$, we can here choose $x = w^{\mathbb{Z}}$ to show that $w^{\mathbb{Z}} \in X'$. To see that w_i $(1 \leq i < n)$ has a unique successor in X', assume to the contrary that $w_i a \in L(X')$ for some $a \in (A \cup A') \setminus \{w_{i+1}\}$. Then in particular there is $x \in X$ such that $w_i a$ occurs in $\psi(x)$ at position 0. But then by definition of ψ, $x[0, n-i] = w_i w_{i+1} \cdots w_n$ and $\psi(x)$ contains an occurrence of $w_i w_{i+1}$ at the origin, contradicting the choice of a. If w is a synchronizing word of X, then from the second item of Lemma 5.2.6 it follows that w is a synchronizing word of X'. $\square$

Lemma 5.2.8. Let $X \subseteq A^{\mathbb{Z}}$ be a subshift and let $A' = \{a' \mid a \in A\}$. Let also $w = w_1 \cdots w_n \in L(X)$ with all $w_i \in A$ distinct be such that w is future deterministic in X. Then there is a conjugacy $\psi : X \to X' \subseteq (A \cup A')^{\mathbb{Z}}$ such that $w \in L(X')$ and w is deterministic in X'. Moreover, if $w^{\mathbb{Z}} \in X$ then $w^{\mathbb{Z}}$ in X', and if w is a synchronizing word of X then w is a synchronizing word of X'.

Proof. Let $\psi : X \to (A \cup A')^{\mathbb{Z}}$ be a morphism defined by

$$\psi(x)[i] = \begin{cases} x[i]' & \text{when } x[i] = w_j \text{ and } x[i-j+1, i] \neq w_1 w_2 \cdots w_j \\ & \text{for some } 1 < j \leq n, \\ x[i] & \text{otherwise.} \end{cases}$$

By Lemma 5.2.6 ψ induces a conjugacy between X and $X' = \psi(X)$. If $x \in X$ contains an occurrence of w at the origin, then $\psi(x)$ also contains an occurrence of w at the origin and $w \in L(X')$. If $w^{\mathbb{Z}} \in X$, we can here choose $x = w^{\mathbb{Z}}$ to show that $w^{\mathbb{Z}} \in X'$. The first item in Lemma 5.2.6 applies to show that w is future deterministic in X', and the same argument as in the proof of the previous lemma shows that w is past deterministic. If w is a synchronizing word of X, then from the second item of Lemma 5.2.6 it follows that w is a synchronizing word of X'. $\square$

Lemma 5.2.9. Let $X \subseteq A^{\mathbb{Z}}$ be a subshift and let $w = w_1 \cdots w_n \in L(X)$ with all w_i distinct. There is an alphabet $B \supseteq A$ and a subshift $X' \subseteq B^{\mathbb{Z}}$ which is conjugate to X such that $w \in L(X')$ and w is deterministic in X'. Moreover, if $w^{\mathbb{Z}} \in X$ then $w^{\mathbb{Z}} \in X'$, and if w is a synchronizing word of X then it is also a synchronizing word of X'.

Proof. This follows by applying the two previous lemmas. $\square$

Definition 5.2.10. The n-th higher power shift $X^{[n]}$ of a subshift $X \subseteq A^{\mathbb{Z}}$ is the image of X under the map $\beta_n(x) : X \to (A^n)^{\mathbb{Z}}$ defined by $\beta_n(x)[i] = x[i-k, i-k+n-1]$ (where $k = \lfloor n/2 \rfloor$) for all $x \in X$, $i \in \mathbb{N}$. All higher power shifts are conjugate to the original subshift.

Lemma 5.2.11. Let $X \subseteq A^{\mathbb{Z}}$ be a nontrivial mixing synchronizing shift. Up to recoding to a conjugate subshift, we may assume there are nonempty words $\mathbf{0}, \mathbf{1} \in L(X)$, $|\mathbf{1}| \geq 2$, such that

- $\mathbf{0}^{\mathbb{Z}} \in X$, $\mathbf{0}$ is deterministic and all symbols of $\mathbf{0}$ are distinct and synchronizing
- none of the symbols of $\mathbf{0}$ occur in $\mathbf{1}$
- $|\mathbf{0}|$ and $|\mathbf{1}|$ are coprime
- $\mathbf{0}\mathbf{1}^*\mathbf{0} \subseteq L(X)$.

Proof. Let $\overline{\mathbf{0}} \in L(X)$ be a nonempty synchronizing word. Since X is nontrivial and mixing, there is a word $w \in L(X)$ with two distinct symbols such that $\overline{\mathbf{0}}w\overline{\mathbf{0}} \in L(X)$ and $\mathbf{0} = \overline{\mathbf{0}}w$ is of prime length. It follows that $\mathbf{0}^{\mathbb{Z}} \in X$ and its minimal period is equal to $|\mathbf{0}|$. For sufficiently large n, $\beta_n(\mathbf{0}^{\mathbb{Z}})[0, |\mathbf{0}|-1]$ is a synchronizing word of $X^{[n]}$ with distinct symbols, so up to conjugacy we may assume that the symbols of $\mathbf{0}$ are distinct. By the previous lemma we may assume up to conjugacy that $\mathbf{0} = 0_1 \cdots 0_p$ ($0_i \in A$) is deterministic in X.

Since X is mixing, there is a word $w \in L(X)$ such that $\mathbf{0}w\mathbf{0} \in L(X)$ and $|w|$ is coprime with $|\mathbf{0}|$. Therefore we may fix a word $w \in L(X)$ of minimal length such that $\mathbf{0}w\mathbf{0} \in L(X)$ and $|w|$ is coprime with $|\mathbf{0}|$ (in particular $|w| \neq 0$ because $|\mathbf{0}| \geq 3$). Then w contains no occurrences of symbols of $\mathbf{0}$, because otherwise $w = w_1\mathbf{0}w_2$ for some $w_1, w_2 \in L(X)$ and $\mathbf{0}w_1\mathbf{0}w_2\mathbf{0} \in L(X)$. Because w is minimal and $|\mathbf{0}|$ is a prime, it follows that $|w_1|, |w_2|$ are divisible by $|\mathbf{0}|$ and then also $|w|$ is divisible by $|\mathbf{0}|$, a contradiction.

Let $A' = \{a' \mid a \in A\}$ and let $\psi : X \to (A \cup A')^{\mathbb{Z}}$ be a morphism defined by

$$\psi(x)[i] = \begin{cases} x[i]' & \text{when } x[i] = 0_j \text{ and } x[i-j-|w|+1, i] = w0_10_2\cdots 0_j \\ x[i] & \text{otherwise.} \end{cases}$$

By Lemma 5.2.6 ψ induces a conjugacy between X and $X' = \psi(X)$. Clearly $\mathbf{0}^{\mathbb{Z}} = \psi(\mathbf{0}^{\mathbb{Z}}) \in X'$, and by Lemma 5.2.6 the word $\mathbf{0}$ is synchronizing and deterministic in X'. Using the fact that $\mathbf{0}$ is deterministic it is easy to show that all symbols of $\mathbf{0}$ are synchronizing. Now denote $\mathbf{0'} = 0_1' \cdots 0_p'$, let $u = w\mathbf{0}$ and $\mathbf{1} = w\mathbf{0}'$. It directly follows that $|\mathbf{1}| \geq 2$ and that none of the symbols of $\mathbf{0}$ occur in $\mathbf{1}$. Since $|w|$ and $|\mathbf{0}|$ are coprime, also $|\mathbf{0}|$ and $|\mathbf{1}|$ are coprime. Since $\mathbf{0}w\mathbf{0} \in L(X)$ and $\mathbf{0}$ is synchronizing in X, it follows that ${}^\infty\mathbf{0}u^*\mathbf{0}^\infty \subseteq X$, and by applying ψ to these points it follows that $\mathbf{0}\mathbf{1}^*\mathbf{0} \subseteq L(X')$. $\square$

In the following we assume that X is a nontrivial mixing synchronizing shift with the words $\mathbf{0}, \mathbf{1} \in L(X)$ as in the statement of the previous lemma. Let $p = |\mathbf{0}|$ and $q = |\mathbf{1}|$. The words

$$\boxed{\leftarrow} = \mathbf{0}^q\mathbf{1} \qquad \boxed{\rightarrow} = \mathbf{1}^{p+1}$$

will be left- and rightbound gliders of a diffusive glider automaton G_X to be defined later. The languages of left- and rightbound gliders are

$$L_\ell = (\boxed{\leftarrow}\mathbf{0}\mathbf{0}^*)^* \qquad L_{\reflectbox{ℓ}} = (\mathbf{0}^*\mathbf{0}\boxed{\rightarrow})^*$$

and we define the glider fleet sets

$$\mathrm{GF}_\ell = {}^\infty\mathbf{0}(\boxed{\leftarrow}\mathbf{0}\mathbf{0}^*)^*\mathbf{0}^\infty \qquad \mathrm{GF}_{\reflectbox{ℓ}} = {}^\infty\mathbf{0}(\mathbf{0}^*\mathbf{0}\boxed{\rightarrow})^*\mathbf{0}^\infty \qquad \mathrm{GF} = \mathrm{GF}_\ell \cup \mathrm{GF}_{\reflectbox{ℓ}}$$

(note that in each element there are only finitely many occurrences of $\boxed{\leftarrow}$ and $\boxed{\rightarrow}$). Elements of $\mathrm{GF} = \mathrm{GF}_\ell \cup \mathrm{GF}_{\reflectbox{ℓ}}$ are called glider fleets.

Earlier we have already used the following simple method of constructing reversible cellular automata: start by defining sliding block codes $F_1, \ldots, F_n$ by telling how they should change occurrences of finite words in configurations, state that they are "clearly well defined and of finite order" (preferably involutive) and in particular reversible and let the final reversible CA be $F_n \circ \cdots \circ F_1$. When the constructions become more complicated, the "clearly" part of this method allows one easily to prove theorems that are not true. For that reason, we now state in Lemma 5.2.13 more explicitly the principle that we will use in this section. This principle is known as the marker method and it has been stated in different sources with varying levels of generality, e.g. for full shifts in [24] and for mixing SFTs in [10]. The statement requires the notion of an overlap.

Definition 5.2.12. Let $u, v \in A^*$. We say that $w \in A^*$ is an *overlap* of u and v if w is a suffix of u and a prefix of v, or if $w = u$ is a subword of v, or if $w = v$ is a subword of u. We say that w is a trivial overlap if $w = \epsilon$ or $w = u = v$.

Lemma 5.2.13. Let X be a subshift, let $u \in L(X)$ and let W be a finite collection of words such that $uWu \subseteq L(X)$ and each pair of (not necessarily distinct) elements of uWu has only u as an overlap in addition to the trivial ones. Let $\pi : uWu \to uWu$ be a permutation that preserves the lengths and syntactic relation classes of elements of uWu. Then there is a reversible CA $F : X \to X$ such that for any $x \in X$ the point $F(x)$ is gotten by replacing every occurrence of any element $w \in uWu$ in x by $\pi(w)$.

Proof. The map F is well defined since the elements of uWu can overlap nontrivially only by u. For the same reason elements of uWu occur in $F(x)$ at precisely the same positions than in x, and then the reversibility of F follows from the reversibility of π. To see that $F(X) \subseteq X$, note first that replacing a single occurrence of a word $uwu \in uWu$ in $x \in X$ by $\pi(uwu)$ yields another configuration from X, because by assumption uwu and $\pi(uwu)$ are in syntactic relation. Then an induction shows that after making any finite number of such replacements the resulting point is still contained in X. From this $F(x) \in X$ follows by compactness because X is a closed subset of $L^1(X)^{\mathbb{Z}}$. $\square$

We now define reversible CA $P_1, P_2 : X \to X$ as follows. In any $x \in X$,

- P_1 replaces every occurrence of $\mathbf{0}(\mathbf{0}^q\mathbf{1})\mathbf{0}$ by $\mathbf{0}(\mathbf{1}^{p+1})\mathbf{0}$ and vice versa.
- P_2 replaces every occurrence of $\mathbf{0}(\mathbf{1}^{p+1})\mathbf{0}$ by $\mathbf{0}(\mathbf{1}\mathbf{0}^q)\mathbf{0}$ and vice versa.

Each P_i is defined as in Lemma 5.2.13 by $u = \mathbf{0}$, a set B_i of two finite words and nontrivial permutations π_i. In each case the words in uB_iu are of equal length and easily verified to have only trivial overlaps by Lemma 5.2.11. By Lemma 5.2.3 both elements in each uB_iu are in syntactic relation, so we conclude that Lemma 5.2.13 is applicable.

For the rest of this section let us assume that $X \subseteq A^{\mathbb{Z}}$ is a mixing sofic shift, so S_X is a finite set. If $\mathbf{0} = 0_1 \cdots 0_p$, denote $B = A \setminus \{0_1, \dots, 0_p\}$. Then also

$$P = \{\mathrm{S}_X(\mathbf{0}w) \mid w \in L(X) \cap B^+, \mathbf{0}w \in L(X), |w| > q(p+1)\}$$

is a finite set and we may choose a uniform $N_1 \in \mathbb{N}$ such that for every $S \in P$ there is a word $w'_S \in L(X) \cap B^+$ with $S = \mathrm{S}_X(\mathbf{0}w'_S)$ and $q(p+1) < |w'_S| \leq N_1$. The set $(\mathbf{10})^+\mathbf{1}^+(\mathbf{1}^{p+1}\mathbf{0})$ contains words of all sufficiently big length, so there is $N \in \mathbb{N}$ such that for every $S \in P$ there is a word $w_S \in (\mathbf{10})^+\mathbf{1}^+(\mathbf{1}^{p+1}\mathbf{0})w'_S$ of length N. In particular $\mathbf{0}w_S \in S$ by Lemma 5.2.3. Fix some such w_S, let $W'_S = \{w_{S,1}, \dots, w_{S,k_S}\}$ be the set of those words from $L(X) \cap B^N$ such that $\mathbf{0}w_{S,i} \in S$ for $1 \leq i \leq k_S$, denote $W_S = W'_S \cup \{w_S\}$ and $W = \bigcup_{S \in P} W_S$. For applying Lemma 5.2.13, let $u = \epsilon$ and let $\pi : \mathbf{0}^{q+1}W \to \mathbf{0}^{q+1}W$ be the permutation that maps the elements of each $\mathbf{0}^{q+1}W_S$ cyclically, i.e. $\mathbf{0}^{q+1}w_S \to \mathbf{0}^{q+1}w_{S,1} \to \cdots \to \mathbf{0}^{q+1}w_{S,k_S} \to \mathbf{0}^{q+1}w_S$. Define the reversible CA $P_3 : X \to X$ that replaces occurrences of elements of $\mathbf{0}^{q+1}W_S$ using the permutation π.

For each $j \in \{1, \dots, p\}$ let $u'_j = \mathbf{1}\mathbf{0}^q\mathbf{1}^j$, and let $U'_j = \{u'_{j,1}, \dots, u'_{j,n_j}\} \subseteq L(X) \cap B^+$ be the set of nonempty words of length at most $N-1$ such that $\mathbf{0}u'_{j,i}\mathbf{0} \in L(X)$, $u'_{j,n_j} = \mathbf{1}^{p+1+j}$ (we can choose N above sufficiently large so that $\left|u'_{j,n_j}\right| < N$), $\left|u'_{j,i}\right| \equiv \left|u'_j\right| \pmod p$, with the additional restriction that $\mathbf{1}, \mathbf{1}^{p+1} \notin U'_p$. Finally, these words are padded to constant length: let $u_j = \mathbf{0}^{c_j} u'_j$ and $u_{j,i} = \mathbf{0}^{c_{j,i}} u'_{j,i}$, where $c_j, c_{j,i} \geq q+1$ are chosen in such a way that all u_j, $u_{j,i}$ are of the same length for any fixed j. Let $U_j = \{u_j\} \cup \{u_{j,i} \mid 1 \leq i \leq n_j\}$, $U = \bigcup_{j=1}^{p} U_j$. For applying Lemma 5.2.13, let $u = \mathbf{0}$, let $V_j, V \subseteq L(X)$ such that $\mathbf{0}V_j\mathbf{0} = U_j\mathbf{0}$, $\mathbf{0}V\mathbf{0} = U\mathbf{0}$ and let $\rho : \mathbf{0}V\mathbf{0} \to \mathbf{0}V\mathbf{0}$ be the permutation that maps the elements of each $\mathbf{0}V_j\mathbf{0}$ cyclically, i.e. $u_j\mathbf{0} \to u_{j,1}\mathbf{0} \to \cdots \to u_{j,n_j}\mathbf{0} \to u_j\mathbf{0}$. Define the reversible CA $P_4 : X \to X$ that replaces occurrences of elements of $U_j\mathbf{0}$ using the permutation ρ.

The *diffusive glider CA* $G_X : X \to X$ is defined as the composition $P_4 \circ P_3 \circ P_2 \circ P_1$.

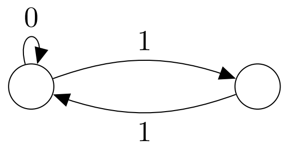

Figure 5.5: The graph of the even shift.

Example 5.2.14. We will give the explicit construction of the diffusive glider CA $G_X : X \to X$ in the case when $X \subseteq \{0,1\}^{\mathbb{Z}}$ is the even shift determined by the collection of forbidden words $\{01^{2n+1}0 \mid n \in \mathbb{N}\}$. More concretely, the configurations of X are precisely the labels of all bi-infinite paths on the graph presented in Figure 5.5. Let $\mathbf{0} = 0$ and $\mathbf{1} = 11$, so $p = |\mathbf{0}| = 1$ and $q = |\mathbf{1}| = 2$. It is easy to verify that these choices of $\mathbf{0}$ and $\mathbf{1}$ satisfy the statement of Lemma 5.2.11 (note in particular that the determinism of $\mathbf{0}$ is vacuously true because $|\mathbf{0}| = 1$). The CA P_1 replaces every occurrence of 000110 by 011110 and vice versa, P_2 replaces every occurrence of 011110 by 011000 and vice versa.

For defining the CA P_3, P_4, note that $B = \{0,1\} \setminus \{0\} = \{1\}$ (the set of symbols not in $\mathbf{0}$) and

$$P = \{\mathrm{S}_X(0w) \mid w \in 1^+, |w| > 4\} = \{\mathrm{S}_X(01^5), \mathrm{S}_X(01^6)\}.$$

Denote $S_0 = \mathrm{S}_X(0) = \mathrm{S}_X(01^6)$ and $S_1 = \mathrm{S}_X(01) = \mathrm{S}_X(01^5)$ and choose $w'_{S_0} = 111111$, $w'_{S_1} = 11111$. Then we can choose

$$\begin{aligned} w_{S_0} &= 110(11)^4 0 w'_{S_0} = 110111111110111111 \text{ and} \\ w_{S_1} &= 110110(11)^3 0 w'_{S_1} = 110110111111011111, \end{aligned}$$

which are of length $N = 18$. If $w \in B^N$ then $w = 1^{18}$ and $\mathrm{S}_X(0w) = S_0$ and therefore $W'_{S_0} = \{w_{S_0,1}\} = \{1^{18}\}$, $W'_{S_1} = \emptyset$ and P_3 is the CA that replaces every occurrence of

$$000w_{S_0} = 000110111111110111111 \text{ by}$$
$$000w_{S_0,1} = 000111111111111111111$$

and vice versa.

Recall that $p = 1$, so u'_j, U'_j, etc. need to be defined only for $j = 1$. Let $u'_1 = 110011$ and $U'_1 = \{u'_{1,i} \mid 1 \leq i \leq 6\}$, where $u'_{1,1} = 1^{16}$, $u'_{1,2} = 1^{14}$, $u'_{1,3} = 1^{12}$, $u'_{1,4} = 1^{10}$, $u'_{1,5} = 1^8$ and $u'_{1,6} = 1^6$. These are padded to constant length: $u_1 = 0^{13}110011$, $u_{1,1} = 0^3 1^{16}$, $u_{1,2} = 0^5 1^{14}$, $u_{1,3} = 0^7 1^{12}$, $u_{1,4} = 0^9 1^{10}$, $u_{1,5} = 0^{11} 1^8$ and $u_{1,6} = 0^{13} 1^6$. are words of length 19. The CA P_4 permutes occurrences of $0^{13}1100110$, $0^3 1^{16} 0$, $0^5 1^{14} 0$, $0^7 1^{12} 0$, $0^9 1^{10} 0$, $0^{11} 1^8 0$ and $0^{13} 1^6 0$ cyclically.

The space-time diagram of a typical finite configuration $x \in X$ with respect to G_X is plotted in Figure 5.6. In this figure it can be seen that x eventually diffuses into two glider fleets, leaving the area around the origin empty.

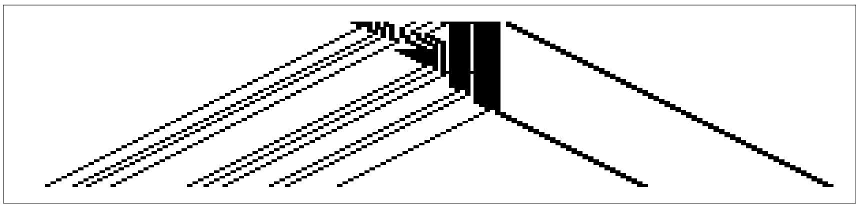

Figure 5.6: Action of $G_X : X \to X$ on a typical $\mathbf{0}$-finite configuration of X when X is the even shift. White and black squares correspond to digits 0 and 1 respectively.

We will prove in Theorem 5.2.19 that the behavior observed in Figure 5.6 also happens in general, thus giving justification for calling G_X a diffusive glider CA. Partial justification is given by the following lemma.

Lemma 5.2.15. If $x \in \mathrm{GF}_\ell$ (resp. $x \in \mathrm{GF}_{\reflectbox{ℓ}}$), then $G_X(x) = \sigma^{pq}(x)$ (resp. $G_X(x) = \sigma^{-pq}(x)$).

Proof. Assume that $x \in \mathrm{GF}_\ell$ (the proof for $x \in \mathrm{GF}_{\reflectbox{ℓ}}$ is similar) and assume that $i \in \mathbb{Z}$ is some position in x where $\boxed{\leftarrow}$ occurs. Then

$$\begin{aligned}
&x[i-p, i+(pq+q)+p-1] = \mathbf{0}\boxed{\leftarrow}\mathbf{0} = \mathbf{0}(\mathbf{0}^q\mathbf{1})\mathbf{0} \\
&P_1(x)[i-p, i+(pq+q)+p-1] = \mathbf{0}(\mathbf{1}^{p+1})\mathbf{0} \\
&P_2(P_1(x))[i-p-pq, i+q+p-1] = \mathbf{0}^q\mathbf{0}(\mathbf{10}) = \mathbf{0}\boxed{\leftarrow}\mathbf{0} \\
&G_X(x) = P_4(P_3(P_2(P_1(x)))) = P_2(P_1(x))),
\end{aligned}$$

so every glider has shifted by distance pq to the left and $G_X(x) = \sigma^{pq}(x)$. $\square$

In fact, the previous lemma would hold even if G_X were replaced by $P_2 \circ P_1$. The role of the part $P_4 \circ P_3$ is, for a given finite point $x \in X$, to "erode" non-$\mathbf{0}$ non-glider parts of x from the left and to turn the eroded parts into new gliders. We will formalize this in a lemma, in the proof of which the following structural definition will be useful.

Definition 5.2.16. Assume that $x \notin \mathrm{GF}_\ell$ is a $\mathbf{0}$-finite element of X not in $\mathcal{O}(\mathbf{0}^{\mathbb{Z}})$. Then there is a maximal $i \in \mathbb{Z}$ such that

$$x[-\infty, i-1] \in {}^{\infty}\mathbf{0}L_\ell,$$

and there is a unique word $w \in \{\mathbf{10}\} \cup \{\mathbf{1}^{p+1}\mathbf{0}\} \cup (\bigcup_{j=1}^{p} U'_j\mathbf{0}) \cup (\bigcup_{S \in P} W'_S)$ such that w is a prefix of $x[i, \infty]$. If $w = \mathbf{1}^{p+1}\mathbf{0}$ or $w \in U'_j\mathbf{0}$, let $k = i + |w| - 1$ and otherwise let $k = i + |\mathbf{10}| - 1$. We say that x is of *left bound type* (w, k) and that it has left bound k (note that $k > i$).

Similarly, if $x \notin \mathrm{GF}_{\not\ell}$ is a non-zero finite element of X, then there is a minimal $k \in \mathbb{Z}$ such that

$$x[k+1, \infty] \in L_{\not\ell}\mathbf{0}^{\infty}$$

and we say that x has right bound k.

We outline a deterministic method to narrow down the word w of the previous definition in a way that clarifies its existence and uniqueness. First, by the maximality of i it follows that $x[i] \in B$. If $x[i, i+N-1] \in B^N$, then $w \in W'_{\mathrm{S}_X(\mathbf{0}x[i,i+N-1])}$ directly by the definition of the sets W'_S. Otherwise $x[i, i+N-1] \notin B^N$ and there is a minimal $m < N$ such that $x[i, i+m-1] \in B^m$ and $x[i+m, i+m+p-1] = \mathbf{0}$. Then $\mathbf{0}x[i, i+m-1]\mathbf{0} \in L(X)$ and $w \in U'_j\mathbf{0}$ for some $j \in \{1, \ldots, p\}$ *unless* we have specifically excluded $x[i, i+m-1]$ from all the sets U'_j. But this happens precisely if $x[i, i+m-1] \in \{\mathbf{1}, \mathbf{1}^{p+1}\}$, in which case $w \in \{\mathbf{10}, \mathbf{1}^{p+1}\mathbf{0}\}$.

The point of this definition is that if x is of left bound type (w, k), then the CA G_X will create a new leftbound glider at position k and break it off from the rest of the configuration.

Lemma 5.2.17. Assume that $x \in X$ has left bound k. Then there exists $t \in \mathbb{N}_+$ such that the left bound of $G_X^t(x)$ is strictly greater than k. Moreover, the left bound of $G_X^{t'}(x)$ is at least k for all $t' \in \mathbb{N}$.

Proof. Let $x \in X$ be of left bound type (w, k) with $w \in \{\mathbf{10}\} \cup \{\mathbf{1}^{p+1}\mathbf{0}\} \cup (\bigcup_{j=1}^{p} U'_j\mathbf{0}) \cup (\bigcup_{S \in P} W'_S)$. The gliders to the left of the occurrence of w near k move to the left at constant speed pq under action of G_X without being affected by the remaining part of the configuration.

Case 1. Assume that $w = \mathbf{1}^{p+1}\mathbf{0}$. Then $P_1(x)[k - (q+2p) + 1, k] = \mathbf{010}$ and we proceed to Case 4.

Case 2. Assume that $w = \mathbf{10}$. Then $x[k-(q+2)p-q+1,k] \neq \mathbf{0}(\mathbf{0}^q\mathbf{1})\mathbf{0} = \mathbf{0}\boxed{\leftarrow}\mathbf{0}$ because otherwise the left bound of x would already be greater than k, so $P_1(x)[k-2p-q+1,k] = \mathbf{010}$ and we proceed to Case 4.

Case 3. Assume that $w = u'_{j,i}\mathbf{0}$ for $1 \leq j \leq p$, $1 \leq i \leq n_j$. There is a minimal $t \in \mathbb{N}$ such that $P_3(P_2(P_1(G_X^t(x))))[k-(p+|u_j|)+1,k] = u_{j,i}\mathbf{0}$. Denote $y = G_X^{t+n_j-i+1}(x)$ so in particular $y[k-(p+|u_j|)+1,k] = u_j\mathbf{0}$. If $j > 1$, then y is of left bound type $(u_{j-1,i'},k)$ for some $1 \leq i' < n_{j-1}$ and we may repeat the argument in this paragraph with a smaller value of j. If $j = 1$, then $P_1(x)[k-(q+2p)+1,k] = \mathbf{010}$ and we proceed as in Case 4.

Case 4. Assume that $P_1(x)[k-(q+2p)+1,k] = \mathbf{010}$. If $P_1(x)[k-(q+2p)+1,k+qp] = \mathbf{0}(\mathbf{10}^q)\mathbf{0}$, then $G_X(x)[k-(q+2p)+1,k+qp] = P_2(P_1(x))[k-(q+2p)+1,k+qp] = \mathbf{01}^{p+1}\mathbf{0}$, $G_X(x)$ is of left bound type $(\mathbf{1}^{p+1}\mathbf{0},k+qp)$ and we are done. Otherwise $P_2(P_1(x))[k-(q+2p)+1,k] = \mathbf{010}$. Denote $y = P_3(P_2(P_1(x)))$. If $y[k-(q+2p)+1,k] \neq \mathbf{010}$, then $G_X(x) = P_4(y)$ is of left bound type $(w_{S,1},k)$ for some $S \in P$ and we proceed as in Case 5. Otherwise $y[k-(q+2p)+1,k] = \mathbf{010}$. If $G_X(x)[k-(q+2p)+1,k] = P_4(y)[k-(q+2p)+1,k] \neq \mathbf{010}$, then $G_X(x)$ is of left bound type $(u_{j,1},k')$ for some $1 \leq j \leq p$, $k' > k$ and we are done. Otherwise $G_X(x)[-\infty,k] \in {}^\infty\mathbf{0}L_\ell$, the left bound of $G_X(x)$ is strictly greater than k and we are done.

Case 5. Assume that $w = w_{S,i}$ for $S \in P$ and $1 \leq i \leq k_S$. Then there is a minimal $t \in \mathbb{N}$ such that $G_X^t(x)[k-|\mathbf{10}|+1,\infty]$ has prefix w_S. Since w_S has prefix $\mathbf{10}$, it follows that $G_X^t(x)[-\infty,k] \in {}^\infty\mathbf{0}L_\ell$. Thus the left bound of $G_X^t(x)$ is strictly greater than k and we are done.

□

Lemma 5.2.18. Assume that $x \in X$ has right bound k. Then there exists $t \in \mathbb{N}_+$ such that the right bound of $G_X^t(x)$ is strictly less than k. Moreover, the right bound of $G_X^{t'}(x)$ is at most k for all $t' \in \mathbb{N}$.

Proof. Let us assume to the contrary that the right bound of $G_X^t(x)$ is at least k for every $t \in \mathbb{N}_+$.

Assume first that the right bound of $G_X^t(x)$ is equal to k for every $t \in \mathbb{N}_+$. By the previous lemma the left bound of $G_X^t(x)$ is arbitrarily large for suitable choice of $t \in \mathbb{N}_+$, which means that for some $t \in \mathbb{N}_+$ $G_X^t(x)$ contains only $\boxed{\leftarrow}$-gliders to the left of $k+3pq$ and only $\boxed{\rightarrow}$-gliders to the right of k. This can happen only if $G_X^t(x)[k+1,k+3pq-1]$ does not contain any glider of either type. Then the right bound of $G_X^{t+1}(x)$ is at most $k-pq$, a contradiction.

Assume then that the right bound of $G_X^t(x)$ is strictly greater than k for some $t \in \mathbb{N}_+$ and fix the minimal such t. This can happen only if $P_1(G_X^{t-1}(x))[k-(p+q)+1, k+(q+1)p] = \mathbf{0}\mathbf{1}\mathbf{0}^q\mathbf{0}$ and then $P_2(P_1(G_X^{t-1}(x)))[k-(p+q)+1, k+(q+1)p] = \mathbf{0}\mathbf{1}^{p+1}\mathbf{0}$. But neither P_3 nor P_4 can change occurrences of $\mathbf{0}\mathbf{1}^{p+1}\mathbf{0}$ in configurations (recall in particular that $|w_S'| > |\mathbf{1}^{p+1}|$ for all $S \in P$) so $G_X^t(x)[k-(p+q)+1, k+(q+1)p] = \mathbf{0}\mathbf{1}^{p+1}\mathbf{0}$. It follows that the right bound of $G_X^t(x)$ is at most $k-(p+q)$, a contradiction. $\square$

By inductively applying the previous lemmas we get the following theorem similarly as in Theorem 5.1.2 and Theorem 5.1.5.

Theorem 5.2.19. If $x \in X$ is a finite configuration, then for every $N \in \mathbb{N}$ there exist $t, N_\ell, N_{\reflectbox{ℓ}}, M \in \mathbb{N}$, $N_\ell, N_{\reflectbox{$\ell$}} \geq N$ such that $G_X^t(x)[-N_\ell, N_{\reflectbox{ℓ}}] = \mathbf{0}^M$, $G_X^t(x)[-\infty, -(N_\ell+1)] \in {}^\infty\mathbf{0}L_\ell$ and $G_X^t(x)[N_{\reflectbox{$\ell$}}+1, \infty] \in L_{\reflectbox{ℓ}}\mathbf{0}^\infty$.

Our construction proves the following theorem. Recall the notions of directional dynamics from Section 2.4.

Theorem 5.2.20. For every nontrivial mixing sofic shift X there exists a reversible CA $F \in \mathrm{Aut}(X)$ that has no almost equicontinuous directions.

Proof. We claim that $G_X : X \to X$ is such an automaton. To see this, assume to the contrary that there is an almost equicontinuous direction r/s for coprime integers r and s such that $s > 0$. This means that $F = \sigma^r \circ G_X^s$ is almost equicontinuous and admits a blocking word $w \in L(X)$. Since every word containing a blocking word is also blocking, we may choose w so that $\mathbf{0}w\mathbf{0} \in L(X)$.

Assume first that $r \geq 0$. Define $x = {}^\infty\mathbf{0}.w\mathbf{0}^\infty$ and $x_n = {}^\infty\mathbf{0}.w\mathbf{0}^n\boxed{\leftarrow}\mathbf{0}^\infty$ for all $n \in \mathbb{N}_+$. We claim that for some $n \in \mathbb{N}_+$ we can choose $t \in \mathbb{N}$ such that $F^t(x)[-\infty, -1] \neq F^t(x_n)[-\infty, -1]$, which would contradict w being a blocking word. To see this, we apply Theorem 5.2.19 for some sufficiently large $N \in \mathbb{N}$ so that $G_X^t(x)[-N_\ell, N_{\reflectbox{ℓ}}] = \mathbf{0}^M$, $G_X^t(x)[-\infty, -(N_\ell+1)] \in {}^\infty\mathbf{0}L_\ell$ and $G_X^t(x)[N_{\reflectbox{$\ell$}}+1, \infty] \in L_{\reflectbox{ℓ}}\mathbf{0}^\infty$ for all t larger than some $t_0 \in \mathbb{N}$, where N_ℓ, $N_{\reflectbox{$\ell$}}$ and M are as in the statement of the theorem. Fix some $i \in \mathbb{N}_+$ such that $G_X^{t_0}(x)[|w|+ip, \infty] = \mathbf{0}^\infty$ and for $j \in \mathbb{N}_+$ let $n_j = j + t_0 q$. Then $x_{n_j} = {}^\infty\mathbf{0}.w\mathbf{0}^{j+t_0q}\boxed{\leftarrow}\mathbf{0}^\infty$ and by fixing $n = n_{i+k}$ for some sufficiently large $k \in \mathbb{N}$ we get $G_X^{t_0}(x_n)[N_{\reflectbox{ℓ}}+1, \infty] \in L_{\reflectbox{ℓ}}\mathbf{0}^*\mathbf{0}^k\boxed{\leftarrow}\mathbf{0}^\infty$. It is possible to choose $t' \geq t_0$ so that $\mathrm{occ}_{\reflectbox{ℓ}}(G_X^{t''}(x_n), \boxed{\leftarrow}) \subseteq (-\infty, -1]$ for all $t'' \geq t'$. Then it holds that $\left|\mathrm{occ}_{\reflectbox{ℓ}}(G_X^{t''}(x_n), \boxed{\leftarrow})\right| > \left|\mathrm{occ}_{\reflectbox{ℓ}}(G_X^{t''}(x), \boxed{\leftarrow})\right|$ for all $t'' \geq t'$. Now let $t \in \mathbb{N}$ such that $st \geq t'$. Then $F^t(x_n) = \sigma^{rt}(G_X^{st}(x_n))$ and $F^t(x) = \sigma^{rt}(G_X^{st}(x))$, so $|\mathrm{occ}_{\reflectbox{ℓ}}(F^t(x_n), \boxed{\leftarrow})| > |\mathrm{occ}_{\reflectbox{ℓ}}(F^t(x), \boxed{\leftarrow})|$. Because we assumed that $r \geq 0$, it also follows that $\mathrm{occ}_{\reflectbox{ℓ}}(F^t(x_n), \boxed{\leftarrow}) \subseteq (-\infty, -1]$ and in particular $F^t(x)[-\infty, -1] \neq F^t(x_n)[-\infty, -1]$.

A symmetric argument yields a contradiction in the case $r \leq 0$. $\square$

Remark 5.2.21. The assumption of X being a sofic shift was used in the construction of G_X only in the definition of the map P_3. The assumption turns out to be essential. In Subsection 5.4.2 we will present a family of synchronizing subshifts on which it is impossible to carry out any construction analogous to that of G_X. Furthermore, on these shifts the previous theorem does not hold.

Problem 5.2.22. Is it possible to generalize the construction of a diffusive glider CA presented in this section to the class of all infinite transitive sofic shifts?

5.3 Application: Finitary Variants of Ryan's Theorem

In this section we discuss an application of the diffusive glider CA construction presented above to the study of the structure of the abstract group $\mathrm{Aut}(X)$. The *centralizer* of a set $S \subseteq \mathcal{M}$ (with respect to a monoid $\mathcal{M}$) is

$$C_{\mathcal{M}}(S) = \{g \in \mathcal{M} \mid g \circ h = h \circ g \text{ for every } h \in S\}.$$

In this section we consider centralizers with respect to some automorphism group $\mathrm{Aut}(X)$ and we drop the subscript from the notation $C_{\mathrm{Aut}(X)}(S)$. The subgroup generated by $S \subseteq \mathrm{Aut}(X)$ is denoted by $\langle S \rangle$. The following definition is by Salo from [53]:

Definition 5.3.1. For a subshift X, let $k(X) \in \mathbb{N} \cup \{\infty, \perp\}$ be the minimal cardinality of a set $S \subseteq \mathrm{Aut}(X)$ such that $C(S) = \langle \sigma \rangle$ if such a set S exists, and $k(X) = \perp$ otherwise.

It is a theorem of Ryan from [49] that $k(A^{\mathbb{Z}}) \neq \perp$, which he later generalized to $k(X) \neq \perp$ whenever X is an infinite transitive SFT in [50]. This result is also presented in Theorem 7.7 of [10] with an alternative proof. An upper bound $k(\Sigma_4^{\mathbb{Z}}) \leq 10$ was given in [53]. Section 7.6 of the same paper contains the following observation concerning the lower bounds of $k(X)$.

Theorem 5.3.2. Let X be a subshift. The case $k(X) = 0$ occurs if and only if $\mathrm{Aut}(X) = \langle \sigma \rangle$. The case $k(X) = 1$ cannot occur.

Proof. The statement $k(X) = 0$ is equivalent to $\langle \sigma \rangle = C(\emptyset) = \mathrm{Aut}(X)$.

The statement $k(X) = 1$ means that $C(\{F\}) = \langle \sigma \rangle$ for some $F \in \mathrm{Aut}(X)$. Because F commutes with itself, it follows that $F = \sigma^i$ for some $i \in \mathbb{Z}$. But all $G \in \mathrm{Aut}(X)$ commute with σ^i and so $\mathrm{Aut}(X) = C(\{F\}) = \langle \sigma \rangle$ and $k(X) = 0$, a contradiction. □

For conjugate subshifts X and Y it necessarily holds that $k(X) = k(Y)$. The quantity $k(X)$ is an isomorphism invariant of the group $\mathrm{Aut}(X)$ and it was suggested in [53] that computing it could theoretically separate $\mathrm{Aut}(X)$ and $\mathrm{Aut}(Y)$ for some mixing SFTs X and Y. Finding good isomorphism invariants of $\mathrm{Aut}(X)$ is of great interest, and it is an open problem whether for example $\mathrm{Aut}(\Sigma_2^{\mathbb{Z}}) \cong \mathrm{Aut}(\Sigma_3^{\mathbb{Z}})$ (Problem 22.1 in [8]). We show that $k(X) = 2$ for all nontrivial mixing sofic shifts (and in particular for all nontrivial mixing SFTs), the proof of which uses our diffusive glider automorphism construction and Lemma 5.3.8.

Lemma 5.3.8 is a criterion saying essentially that if S is a collection of automorphisms that acts together with the diffusive glider CA G in a special way, then $C(S \cup \{G\})$ is not very complicated. A special case occurs as part of the proof of Theorem 14 in [37]. We have formulated a reasonably general version of the lemma to allow its application in other contexts. To state the lemma we also have to give a general definition of diffusive glider CA.

Definition 5.3.3. Given a subshift $X \subseteq A^{\mathbb{Z}}$, an *abstract glider automorphism group* is any tuple $(\mathcal{G}, \mathbf{0}, \mathcal{I}, \mathrm{spd}, \varsigma, \mathrm{GF})$ (or just $\mathcal{G}$ when the rest of the tuple is clear from the context) where $\mathcal{G} \subseteq \mathrm{Aut}(X)$ is a subgroup, $\mathcal{I}$ is an index set, $\mathbf{0} \in A^+$ and

- $\mathrm{spd} : \mathcal{I} \to \mathbb{Z}$ is called a *speed map* and $\varsigma : \mathcal{I} \to \mathcal{G}$ (image at $i \in \mathcal{I}$ is denoted by ς_i) is called a *local shift map*
- GF is a map from $\mathcal{I}$ to subsets of X whose image at $i \in \mathcal{I}$ is

  $$\mathrm{GF}_i = \{x \in X \mid x \text{ is } \mathbf{0}\text{-finite and } \varsigma_i(x) = \sigma^{\mathrm{spd}(i)}(x)\} \supsetneq \mathcal{O}(\mathbf{0}^{\mathbb{Z}})$$

  and is called a *glider fleet set*. Elements of GF_i are called glider fleets.

This tuple is an abstract *diffusive* glider automorphism group if in addition

- for every $\mathbf{0}$-finite $x \in X$ and every $N \in \mathbb{N}$ there is a $G \in \mathcal{G}$ such that for every $i \in \mathbb{Z}$, $G(x)[i, i+N] \in L(\mathrm{GF}_j)$ for some $j \in \mathcal{I}$.

If $\mathcal{G}$ is generated by a single automorphism $G \in \mathrm{Aut}(X)$, we say that G is an *abstract (diffusive) glider CA*.

The idea of an abstract diffusive glider automorphism group is the following. For any $\mathbf{0}$-finite $x \in X$ there is a $G \in \mathcal{G}$ that can be used to "diffuse" x into a point $G(x)$ such that the elements of $\mathcal{O}(G(x))$ locally look like elements of some GF_i, and in practice $\overline{\mathrm{GF}_i}$ will be in some sense simpler subshifts than X. The local shift maps ς_i are used to dynamically distinguish the points in $\mathrm{GF}_i \setminus \mathcal{O}(\mathbf{0}^{\mathbb{Z}})$. In the proof Lemma 5.3.8 we will also require that the points of GF_i consist of gliders in a more concrete sense. We encode this in the following definition.

Definition 5.3.4. Given a subshift $X \subseteq A^{\mathbb{Z}}$, a *(diffusive) glider automorphism group* is any tuple $(\mathcal{G}, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ (or just $\mathcal{G}$ when the rest of the tuple is clear from the context) where $(\mathcal{G}, \mathbf{0}, \mathcal{I}, \mathrm{spd}, \varsigma, \mathrm{GF})$ is an abstract (diffusive) glider automorphism group and

- $\boxed{\leftrightarrow} : \mathcal{I} \to A^{+}$ is a map whose image at $i \in \mathcal{I}$ is denoted by $\boxed{\leftrightarrow}_i$ and is called a *glider*
- for every $i \in \mathcal{I}$ there is some $n \in \mathbb{N}$ such that $\mathrm{GF}_i = {}^{\infty}\mathbf{0}(\boxed{\leftrightarrow}_i \mathbf{0}^n \mathbf{0}^*)^* \mathbf{0}^{\infty}$: note that these configurations are $\mathbf{0}$-finite
- for every $i \in \mathcal{I}$ and $x \in \mathrm{GF}_i$ it holds that $|j - k| \geq |\boxed{\leftrightarrow}_i|$ whenever $j, k \in \mathrm{occ}_{\ell}(x, \boxed{\leftrightarrow}_i)$ are distinct, i.e. the occurrences of $\boxed{\leftrightarrow}_i$ do not overlap in any point of GF_i.

If $\mathcal{G}$ is generated by a single automorphism $G \in \mathrm{Aut}(X)$, we say that G is a *(diffusive) glider CA*.

Example 5.3.5. We consider a partial shift $\tau : (\Sigma_2 \times \Sigma_2)^{\mathbb{Z}} \to (\Sigma_2 \times \Sigma_2)^{\mathbb{Z}}$ defined by $\tau(x_1, x_2) = (\sigma(x_1), x_2)$ for all $x_1, x_2 \in \Sigma_2^{\mathbb{Z}}$ (recall that this is the CA of Figure 5.1 up to a bijection between the alphabets $\Sigma_2 \times \Sigma_2$ and Σ_4). Denote $A = \Sigma_2 \times \Sigma_2$. The map τ is a diffusive glider CA with an associated diffusive glider automorphism group $(\mathcal{G}, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ where $\mathcal{G} = \langle \tau \rangle$, $\mathbf{0} = (0, 0) \in A$, $\mathcal{I} = \{0, 1\}$, $\boxed{\leftrightarrow}_0 = (0, 1) \in A$, $\boxed{\leftrightarrow}_1 = (1, 0) \in A$, $\mathrm{spd}(i) = i$, $\varsigma_i = \tau$ (for $i \in \mathcal{I}$) and GF_0 (resp. GF_1) consists of those $\mathbf{0}$-finite points $x = (x_1, x_2) \in \Sigma_2^{\mathbb{Z}} \times \Sigma_2^{\mathbb{Z}}$ such that x_1 (resp. x_2) contains no occurrences of the digit 1.

Example 5.3.6. Let Y be a nontrivial mixing sofic shift. In the previous section we found a conjugate subshift X on which we constructed the diffusive glider CA $G_X : X \to X$. We claim that this really is a diffusive glider CA in the sense of Definition 5.3.4 with an associated glider automorphism group $(\langle G_X \rangle, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ defined as follows. Let $p, q, \mathbf{0}, \boxed{\leftarrow}, \boxed{\rightarrow}, \mathrm{GF}$ be as in the construction of the previous section. Let $\mathcal{I} = \{\ell, \reflectbox{ℓ}\}$, $\mathrm{spd}(\ell) = pq$, $\mathrm{spd}(\reflectbox{ℓ}) = -pq$ and $\varsigma_{\ell} = \varsigma_{\reflectbox{ℓ}} = G_X$. Let $\boxed{\leftrightarrow}_{\ell} = \boxed{\leftarrow}$, $\boxed{\leftrightarrow}_{\reflectbox{ℓ}} = \boxed{\rightarrow}$. The fleets GF_{ℓ} and $\mathrm{GF}_{\reflectbox{ℓ}}$ are as in the previous section.

By Lemma 5.2.15 we know that for $i \in \mathcal{I}$,

$$\mathrm{GF}_i \subseteq \{x \in X \mid x \text{ is } \mathbf{0}\text{-finite and } G_X(x) = \sigma^{\mathrm{spd}(i)}(x)\} \doteqdot S_i.$$

We prove the other inclusion when $i = \ell$, the case $i = \reflectbox{$\ell$}$ being similar. Assume therefore that $x \notin \mathrm{GF}_{\ell}$ is $\mathbf{0}$-finite and apply Theorem 5.2.19 for sufficiently large M. By Lemma 5.2.15 the set GF_i is invariant under the map G_X, so $G_X^t(x) \notin \mathrm{GF}_{\ell}$ and $G_X^t(x)$ contains an occurrence of $\boxed{\rightarrow}$ which is shifted to the right by the map G_X. Therefore $G_X(G_X^t(x)) \neq \sigma^{pq}(G_X^t(x)) =$

$\sigma^{\mathrm{spd}(\ell)}(G_X^t(x))$ and $G_X^t(x) \notin S_\ell$. Since S_ℓ is invariant under the map G_X, it follows that $x \notin S_\ell$.

The other conditions necessary for showing that G_X is a glider CA are easy to check. Then the fact that G_X is a diffusive glider CA follows from Theorem 5.2.19.

Since X and Y are conjugate, there is a conjugacy $\psi : Y \to X$ and it is straightforward to see that $\psi^{-1} \circ G_X \circ \psi : Y \to Y$ is an abstract diffusive glider CA on Y.

In the next lemma we need the notion of a bipartite non-directed graph. By this we mean a pair $\mathcal{B} = (V, E)$ where V is the set of vertices with a nontrivial partition $V = V_1 \cup V_2$ and $E \subseteq V_1 \times V_2$ is the set of edges, i.e. an edge cannot connect two vertices belonging in the same element of the partition. V and E are not necessarily finite. We say that $\mathcal{B}$ is connected if the equivalence relation on V generated by E is equal to $V \times V$, which is equivalent to saying that it is possible to traverse between any two vertices by a finite path in which edges can be crossed in both directions.

We also require the notion of an automorphism that fixes the orbit of a given periodic point in a given subshift.

Definition 5.3.7. For a subshift $X \subseteq A^{\mathbb{Z}}$ and a word $w \in A^+$ such that $w^{\mathbb{Z}} \in X$ denote $\mathrm{Aut}(X, w) = \{F \in \mathrm{Aut}(X) \mid F(\mathcal{O}(w^{\mathbb{Z}})) = \mathcal{O}(w^{\mathbb{Z}})\}$.

Lemma 5.3.8. Let $X \subseteq A^{\mathbb{Z}}$ be a subshift with a diffusive glider automorphism group $(\mathcal{G}, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ such that $\mathbf{0}$-finite configurations are dense in X. Let $\mathcal{I}_1 \cup \mathcal{I}_2 = \mathcal{I}$ be a nontrivial partition and let $\mathcal{B} = (\mathcal{I}, E)$ be a bipartite non-directed graph with an edge from $i \in \mathcal{I}_1$ to $j \in \mathcal{I}_2$ if and only if there are $d, e \in \mathbb{N}_+$, a strictly increasing sequence $(N_m)_{m\in\mathbb{N}} \in \mathbb{N}^{\mathbb{N}}$ and $(G_m)_{m\in\mathbb{N}} \in \mathcal{G}^{\mathbb{N}}$ such that for any $x\boxed{\leftrightarrow}_i\mathbf{0}^\infty \in \mathrm{GF}_i$, ${}^\infty\mathbf{0}\boxed{\leftrightarrow}_j y \in \mathrm{GF}_j$ we have

- $x\boxed{\leftrightarrow}_i.\mathbf{0}^{N_m}\boxed{\leftrightarrow}_j y \in X$
- $G_m(x\boxed{\leftrightarrow}_i.\mathbf{0}^N\boxed{\leftrightarrow}_j y) = x\boxed{\leftrightarrow}_i\mathbf{0}^d.\mathbf{0}^N\mathbf{0}^e\boxed{\leftrightarrow}_j y$ for every $N > N_m$ such that $x\boxed{\leftrightarrow}_i.\mathbf{0}^N\boxed{\leftrightarrow}_j y \in X$
- $G_m(x\boxed{\leftrightarrow}_i.\mathbf{0}^{N_m}\boxed{\leftrightarrow}_j y) = x\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^{N_m}\boxed{\leftrightarrow}_j\mathbf{0}^e y$.

If $\mathcal{B}$ is connected then $C(\mathcal{G}) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle\sigma\rangle$.

Before the proof we continue our earlier example and show how this lemma can be applied to it.

Example 5.3.9. We use the notation of Example 5.3.5. Furthermore, we denote $\boxed{\leftarrow} = \boxed{\leftrightarrow}_1$ and $\boxed{} = \boxed{\leftrightarrow}_0$ to reflect the fact that occurrences $\boxed{\leftarrow}$ move to the left and occurrences of $\boxed{}$ remain stationary under the action of the map τ. Note that $(\mathcal{G}, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ remains a diffusive glider automorphism group even when $\mathcal{G}$ is replaced by a larger group $\mathcal{G}' \supseteq \mathcal{G}$. We let $\mathcal{G}' = \langle \tau, F, \sigma \rangle$ where $F = F_2 \circ F_1$ for automorphisms $F_1, F_2 : X \to X$ such that

- F_1 replaces every occurrence of $(0,1)(0,0)(0,0)(1,0) = \boxed{}\mathbf{00}\boxed{\leftarrow}$ by $(0,1)(0,0)(1,0)(0,0) = \boxed{}\mathbf{0}\boxed{\leftarrow}\mathbf{0}$ and vice versa

- F_2 replaces every occurrence of $(0,1)(0,0)(1,0) = \boxed{}\mathbf{0}\boxed{\leftarrow}$ by $(0,0)(0,1)(1,0) = \mathbf{0}\boxed{}\boxed{\leftarrow}$ and vice versa.

The map F has two important properties. First, it replaces any occurrence of $\boxed{}\mathbf{00}\boxed{\leftarrow}$ by $\mathbf{0}\boxed{}\boxed{\leftarrow}\mathbf{0}$. Second, if $x \in X$ is a configuration containing only gliders $\boxed{}$ and $\boxed{\leftarrow}$ separated by words from $\mathbf{0}^*$ and if every occurrence of $\boxed{}$ is sufficiently far from every occurrence of $\boxed{\leftarrow}$, then $F(x) = x$.

We use the lemma to show that $C(\mathcal{G}') \cap \mathrm{Aut}(X, \mathbf{0}) = \langle \sigma \rangle$. The bipartite graph $\mathcal{B}$ in the statement of the lemma has in this case the set of vertices $\{0, 1\}$ with the partition $\mathcal{I}_1 = \{0\}$ and $\mathcal{I}_2 = \{1\}$, so it suffices to show that there is an edge between 0 and 1.

Still using the same notation as in the statement of the lemma, let $d = e = 1$, $(N_m)_{m \in \mathbb{N}}$ with $N_m = 2+m$ and $(G_m)_{m \in \mathbb{N}}$ with $G_m = \sigma \circ \tau^{-(m+2)} \circ F \circ \tau^m$. Let $x\boxed{}\mathbf{0}^\infty \in \mathrm{GF}_0 = {}^\infty\mathbf{0}\{\mathbf{0}, \boxed{}\}^*\mathbf{0}^\infty$, ${}^\infty\mathbf{0}\boxed{\leftarrow}y \in \mathrm{GF}_1 = {}^\infty\mathbf{0}\{\mathbf{0}, \boxed{\leftarrow}\}^*\mathbf{0}^\infty$ be arbitrary. Fix some $m \in \mathbb{N}$. Since X is a full shift, it is clear that $x\boxed{}.\mathbf{0}^{N_m}\boxed{\leftarrow}y \in X$ and it is easy to verify that

- $G_m(x\boxed{}.\mathbf{0}^N\boxed{\leftarrow}y) = x\boxed{}\mathbf{0}.\mathbf{0}^N\mathbf{0}\boxed{\leftarrow}y$ for $N > N_m$

- $G_m(x\boxed{}.\mathbf{0}^{N_m}\boxed{\leftarrow}y) = x\mathbf{0}\boxed{}.\mathbf{0}^{N_m}\boxed{\leftarrow}\mathbf{0}y$.

It follows that there is an edge between 0 and 1, so $C(\mathcal{G}') \cap \mathrm{Aut}(X, \mathbf{0}) = \langle \sigma \rangle$. In other words, if $H \in \mathrm{Aut}(X)$ has $0^{\mathbb{Z}}$ as a fixed point and if it commutes with both F and τ (and σ, but this holds for all elements of $\mathrm{Aut}(X)$), then $H = \sigma^i$ for some $i \in \mathbb{Z}$.

In this example we augmented $\mathcal{G}$ by an automorphism F (and by σ) and got a group $\mathcal{G}'$ satisfying the assumptions of Lemma 5.3.8. The construction of such a map F will be essentially the same in all our later applications of the lemma. To gain a better understanding of the lemma, it may be helpful to consider how the following proof would go in the case of the previous example.

Proof of Lemma 5.3.8. Assume that $F \in C(\mathcal{G}) \cap \mathrm{Aut}(X, \mathbf{0})$ is a radius-r automorphism whose inverse is also a radius-r automorphism. Since we aim to prove that $F \in \langle \sigma \rangle$, we lose no generality by transforming F throughout the proof by taking inverses and composing it with some shift. We start by noting that without loss of generality (by composing F with a suitable power of σ if necessary) $\mathbf{0}^{\mathbb{Z}}$ is a fixed point of F.

We have that $F(\mathrm{GF}_i) \subseteq \mathrm{GF}_i$ for $i \in \mathcal{I}$. To see this, assume to the contrary that $x \in \mathrm{GF}_i$ but $F(x) \notin \mathrm{GF}_i$. Then $F(\varsigma_i(x)) = F(\sigma^{\mathrm{spd}(i)}(x)) = \sigma^{\mathrm{spd}(i)}(F(x)) \neq \varsigma_i(F(x))$, contradicting the assumption $F \in C(\mathcal{G})$.

For all $i \in \mathcal{I}_1$, $j \in \mathcal{I}_2$ and all $x_1 \in \mathrm{GF}_i$ and $x_2 \in \mathrm{GF}_j$ not in $\mathcal{O}(\mathbf{0}^{\mathbb{Z}})$ we define the right and left offsets

$$\begin{aligned}
\mathrm{off}_{\reflectbox{ℓ}}(x_1) &= \max\{\mathrm{occ}_{\reflectbox{ℓ}}(F(x_1), \boxed{\leftrightarrow}_i)\} - \max\{\mathrm{occ}_{\reflectbox{ℓ}}(x_1, \boxed{\leftrightarrow}_i)\},\\
\mathrm{off}_{\ell}(x_2) &= \min\{\mathrm{occ}_{\ell}(F(x_2), \boxed{\leftrightarrow}_j)\} - \min\{\mathrm{occ}_{\ell}(x_2, \boxed{\leftrightarrow}_j)\}.
\end{aligned}$$

We claim that $\mathrm{off}_{\ell}(x_2) - \mathrm{off}_{\reflectbox{ℓ}}(x_1) = 0$. To see this, assume to the contrary that this does not hold. Since $\mathcal{B}$ is connected, there is a path from i to j, along which there is an edge from $i' \in \mathcal{I}_1$ to $j' \in \mathcal{I}_2$ and some $x_1' \in \mathrm{GF}_{i'}$, $x_2' \in \mathrm{GF}_{j'}$ not in $\mathcal{O}(\mathbf{0}^{\mathbb{Z}})$ such that $\mathrm{off}_{\ell}(x_2') - \mathrm{off}_{\reflectbox{ℓ}}(x_1') \neq 0$. Then we can assume without loss of generality that $\mathrm{off}_{\reflectbox{ℓ}}(x_1') = 0$ (by replacing F with $F \circ \sigma^{\mathrm{off}_{\reflectbox{ℓ}}(x_1')}$ if necessary), that $\mathrm{off}_{\ell}(x_2') > 0$ (by replacing F with F^{-1}, x_1' with $F(x_1')$ and x_2' with $F(x_2')$ if necessary) and that $\min\{\mathrm{occ}_{\ell}(x_2', \boxed{\leftrightarrow}_j)\} = N_m$, $\max\{\mathrm{occ}_{\reflectbox{ℓ}}(x_1', \boxed{\leftrightarrow}_i)\} = -1$ with $m \in \mathbb{N}$ such that $N_m \geq 2r+1$ (by shifting x_1' and x_2' suitably). Then consider $x = x_1' \otimes x_2'$ and note that $F(x) = F(x_1') \otimes F(x_2')$ by the choice of N_m. By our assumption on offsets and the map G_m it follows that

$$\begin{aligned}
F^{-1}&(G_m(F(x))) = F^{-1}(\sigma^{|\mathbf{0}|d}(F(x_1')) \otimes \sigma^{-|\mathbf{0}|e}(F(x_2')))\\
&= \sigma^{|\mathbf{0}|d}(x_1') \otimes \sigma^{-|\mathbf{0}|e}(x_2') \neq G_m(x)
\end{aligned}$$

and thus $G_m \circ F \neq F \circ G_m$, contradicting the assumption $F \in C(\mathcal{G})$. In the following we may therefore assume that $\mathrm{off}_{\ell}(x_2) = \mathrm{off}_{\reflectbox{ℓ}}(x_1) = 0$ for all $i \in \mathcal{I}_1$, $j \in \mathcal{I}_2$ and all $x_1 \in \mathrm{GF}_i$ and $x_2 \in \mathrm{GF}_j$ not in $\mathcal{O}(\mathbf{0}^{\mathbb{Z}})$.

If $x \in \mathrm{GF}_i$ is a configuration containing exactly one occurrence of $\boxed{\leftrightarrow}_i$, then $F(x) = x$. To see this, assume to the contrary (without loss of generality), that $F(x)$ contains at least two occurrences of $\boxed{\leftrightarrow}_i$, that $i \in \mathcal{I}_1$ (the case $i \in \mathcal{I}_2$ being similar), that $y \in \mathrm{GF}_j$ is a configuration containing a single $\boxed{\leftrightarrow}_j$ for j such that there is an edge from i to j in $\mathcal{B}$ and that $\min\{\mathrm{occ}_{\ell}(y, \boxed{\leftrightarrow}_j)\} = N_m$, $\max\{\mathrm{occ}_{\reflectbox{ℓ}}(x, \boxed{\leftrightarrow}_i)\} = -1$ with $m \in \mathbb{N}$ such that $N_m \geq 2r+1$ (by shifting x and y suitably). Then consider $z = x \otimes y$ and note that $G_m(z) = z$ but $G_m(F(z)) \neq F(z)$ because G_m at least shifts the leftmost glider in $F(z)$. Thus $F(G_m(z)) = F(z) \neq G_m(F(z))$, contradicting the assumption $F \in C(\mathcal{G})$.

Now let us prove that if $x \in \mathrm{GF}_i$, then $F(x) = x$. To see this, assume to the contrary that $F(x) \neq x$, that $i \in \mathcal{I}_1$ (the case $i \in \mathcal{I}_2$ being similar), that x contains a minimal number of occurrences of $\boxed{\leftrightarrow}_i$ (at least two by the previous paragraph) and that the distance from the rightmost $\boxed{\leftrightarrow}_i$ to the second-to-rightmost $\boxed{\leftrightarrow}_i$ in x is maximal. Let $y \in \mathrm{GF}_j$ be a configuration containing a single $\boxed{\leftrightarrow}_j$ for j such that there is an edge from i to j in $\mathcal{B}$ and assume that $\min\{\mathrm{occ}_\ell(y, \boxed{\leftrightarrow}_j)\} = N_m$, $\max\{\mathrm{occ}_{\reflectbox{ℓ}}(x, \boxed{\leftrightarrow}_i)\} = -1$ with $m \in \mathbb{N}$ such that $N_m \geq 2r + 1$ (by shifting x and y suitably). Then $x[-\infty, -1], F(x)[-\infty, -1]$ are of the form $z_1\boxed{\leftrightarrow}_i, z_2\boxed{\leftrightarrow}_i \in {}^\infty\mathbf{0}L(\mathrm{GF}_i)$ with $z_1 \neq z_2$. Consider $z = x \otimes y$ and note that

$$
\begin{aligned}
&G_m(z)[-\infty, -1] = z_1\mathbf{0}^d\boxed{\leftrightarrow}_i \\
&F(G_m(z))[-\infty, -1] = G_m(F(x))[-\infty, -1] = z_2\mathbf{0}^d\boxed{\leftrightarrow}_i.
\end{aligned}
$$

It follows that

$$
F(z_1\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^\infty) = z_2\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^\infty \neq z_1\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^\infty,
$$

contradicting the maximal distance between the two rightmost occurrences of $\boxed{\leftrightarrow}_i$ in x.

If x is a $\mathbf{0}$-finite configuration, then $F(x) = x$. Namely, let $N \geq 2r + 1$, and because $\mathcal{G}$ is a diffusive glider automorphism group of X, there exists $G \in \mathcal{G}$ such that for every $i \in \mathbb{Z}$, $G(x)[i, i + N] \in L(\mathrm{GF}_j)$ for some $j \in \mathcal{I}$. Because F acts like the identity on all GF_j, it follows that $F(G(x)) = G(x)$. By using the assumption $F \in C(\mathcal{G})$ it follows that

$$
F(x) = F(G^{-1}(G(x))) = G^{-1}(F(G(x))) = G^{-1}(G(x)) = x.
$$

Finally, because F is a continuous map that agrees with the identity map on the dense set of $\mathbf{0}$-finite configurations, it follows that F is the identity map and in particular $F \in \langle \sigma \rangle$. □

5.3.1 Finitary Ryan's Theorem for Mixing Sofic Shifts

In this section we prove our finitary version of Ryan's theorem. This is done by applying Lemma 5.3.8. As in Example 5.3.9, we need a suitable automorphism F to augment the diffusive glider automorphism group of Example 5.3.6.

As earlier, let X be a mixing sofic shift of the form given in Lemma 5.2.11 and consider the notation of Section 5.2. First we define maps $F_1, F_2 : X \to X$ as follows. In any $x \in X$,

- F_1 replaces every occurrence of $\mathbf{0}\boxed{\rightarrow}\mathbf{000}\boxed{\leftarrow}\mathbf{0}$ by $\mathbf{0}\boxed{\rightarrow}\mathbf{00}\boxed{\leftarrow}\mathbf{00}$ and vice versa

- F_2 replaces every occurrence of $\mathbf{0}\boxed{\rightarrow}\mathbf{00}\boxed{\leftarrow}\mathbf{0}$ by $\mathbf{00}\boxed{\rightarrow}\mathbf{0}\boxed{\leftarrow}\mathbf{0}$ and vice versa.

It is easy to see that these maps are well-defined automorphisms of X. The automorphism $F : X \to X$ is then defined as the composition $F_2 \circ F_1$. Similarly to Example 5.3.9, F has the following properties. First, it replaces any occurrence of $\mathbf{0}\boxed{\rightarrow}\mathbf{000}\boxed{\leftarrow}\mathbf{0}$ by $\mathbf{00}\boxed{\rightarrow}\mathbf{0}\boxed{\leftarrow}\mathbf{00}$. Second, if $x \in X$ is a configuration containing only gliders $\boxed{\leftarrow}$ and $\boxed{\rightarrow}$ separated by words from $\mathbf{0}^+$ and if every occurrence of $\boxed{\leftarrow}$ is sufficiently far from every occurrence of $\boxed{\rightarrow}$, then $F(x) = x$.

Proposition 5.3.10. Let $X \subseteq A^{\mathbb{Z}}$ and $G_X, F : X \to X$ be as above. Then $C(\langle G_X, F\rangle) = \langle \sigma \rangle$.

Proof. Let $(\langle G_X\rangle, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ be the diffusive glider automorphism group from Example 5.3.6. If we define $\mathcal{G} = \langle G_X, F\rangle$, then it directly follows that $(\mathcal{G}, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ is also a diffusive glider automorphism group of X. We want to use Lemma 5.3.8 to show that $C(\mathcal{G}) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle \sigma \rangle$. The bipartite graph $\mathcal{B}$ in the statement of the lemma has in this case the set of vertices $\mathcal{I} = \{r, \ell\}$ with the partition $\mathcal{I}_1 = \{r\}$ and $\mathcal{I}_2 = \{\ell\}$, so it suffices to show that there is an edge between r and ℓ.

Recall that we denote $p = |\mathbf{0}|$, $q = |\mathbf{1}|$. Using the same notation as in the statement of Lemma 5.3.8, let $d = e = 1$, $(N_m)_{m\in\mathbb{N}}$ with $N_m = 2mq + 3$ and $(G_m)_{m\in\mathbb{N}}$ with $G_m = G_X^{-(m+1)} \circ F \circ G_X^m$. Let $x\boxed{\rightarrow} \in {}^{\infty}\mathbf{0}L_r$, $\boxed{\leftarrow}y \in L_\ell \mathbf{0}^{\infty}$ be arbitrary. Fix some $m \in \mathbb{N}$. Since $\mathbf{0}$ is synchronizing in X, it is clear that $x\boxed{\rightarrow}.\mathbf{0}^{N_m}\boxed{\leftarrow}y \in X$ and it is easy to verify that

- $G_m(x\boxed{\rightarrow}.\mathbf{0}^N\boxed{\leftarrow}y) = x\boxed{\rightarrow}\mathbf{0}.\mathbf{0}^N\mathbf{0}\boxed{\leftarrow}y$ for $N > N_m$
- $G_m(x\boxed{\rightarrow}.\mathbf{0}^{N_m}\boxed{\leftarrow}y) = x\mathbf{0}\boxed{\rightarrow}.\mathbf{0}^{N_m}\boxed{\leftarrow}\mathbf{0}y$.

It follows that there is an edge between r and ℓ, so $C(\mathcal{G}) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle \sigma \rangle$.

Now let $H \in C(\mathcal{G})$ be arbitrary. Let us show that $H \in \mathrm{Aut}(X, \mathbf{0})$. Namely, assume to the contrary that $H(\mathbf{0}^{\mathbb{Z}}) = w^{\mathbb{Z}} \notin \mathcal{O}(\mathbf{0}^{\mathbb{Z}})$ for some $w = w_1 \cdots w_p$ $(w_i \in A)$. The maps P_k in the definition of G_X have been defined so that $P_k(x)[i] = x[i]$ whenever x contains occurrences of $\mathbf{0}$ only at positions strictly greater than i, so in particular $G_X(w^{\mathbb{Z}}) = w^{\mathbb{Z}}$. Consider $x = {}^{\infty}\mathbf{0}.\boxed{\leftarrow}\mathbf{0}^{\infty} \in \mathrm{GF}_\ell$ with the glider $\boxed{\leftarrow}$ at the origin. Note that $H(x)[(i-1)p, ip-1] \neq w$ for some $i \in \mathbb{Z}$ (otherwise $H(x) = w^{\mathbb{Z}} = H(\mathbf{0}^{\mathbb{Z}})$, contradicting the injectivity of H) and $H(x)[-\infty, ip-(jq)p-1] = \cdots www$ for some $j \in \mathbb{N}_+$. By the earlier observation on the maps P_k it follows that $G_X^t(H(x))[-\infty, ip-(jq)p-1] = \cdots www$ for every $t \in \mathbb{Z}$ but $H(G_X^j(x))[ip-(j+1)qp, ip-(jq)p-1] = H(\sigma^{(pq)j}(x))[ip-(j+1)qp, ip-(jq)p-1] = H(x)[ip-qp, ip-1] \neq w^q$, contradicting the commutativity of H and G_X. Thus $H \in \mathrm{Aut}(X, \mathbf{0})$.

We have shown that $H \in C(\mathcal{G}) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle \sigma \rangle$, so we are done. ☐

Theorem 5.3.11 (Finitary Ryan's theorem)**.** $k(X) = 2$ for every nontrivial mixing sofic shift X.

Proof. Every nontrivial mixing sofic shift is conjugate to a subshift X of the form given in Lemma 5.2.11, so $k(X) \leq 2$ follows from the previous proposition. Clearly $\mathrm{Aut}(X) \neq \langle\sigma\rangle$, so by Theorem 5.3.2 it is not possible that $k(X) < 2$ and therefore $k(X) = 2$. $\square$

Corollary 5.3.12. $k(X) = 2$ for every transitive SFT X which is not the orbit of a single point.

Proof. Let X be a transitive SFT given as the edge subshift of a graph $\mathcal{G} = (V, E)$ containing more than a single cycle. By Section 4.5 in [43] there is a partition $E = \bigcup_{i=1}^{n} E_n$ with the following properties. First, the ending states of E_i can be starting states only for edges of E_{i+1} (where $i + 1$ is considered modulo n) and this induces a partition $X = \bigcup_{i=1}^{n} X_i$ such that $X_i = \{x \in X \mid x[0] \in E_i\}$ and $\sigma(X_i) = X_{i+1}$. Second, the edge shift X' of the graph $\mathcal{G}' = (V', E')$ is a nontrivial mixing SFT where $V' \subseteq V$ contains the starting states of edges in E_1 and E' contains all paths $w = w_1 \cdots w_n$ of length n in $\mathcal{G}$ with $w_1 \in E_1$ and we let $\iota(w) = \iota(w_1)$, $\tau(w) = \tau(w_n)$. There is a natural homeomorphism $\phi : X' \to X_1$ such that $\phi \circ \sigma = \sigma^n \circ \phi$. By the previous theorem there are $F_1', F_2' \in \mathrm{Aut}(X')$ which commute with only $\langle\sigma_{X'}\rangle$ and there are unique $F_1, F_2 \in \mathrm{Aut}(X)$ such that $F_{i\restriction X_1} = \phi \circ F_i' \circ \phi^{-1}$. By Theorem 5.3.2 it remains to show that $C(\{F_1, F_2\}) = \langle\sigma\rangle$. Assume therefore that H commutes with F_1 and F_2 and without loss of generality (by composing H with some power of σ_X if necessary) that $H(X_1) = X_1$. There is $H' \in \mathrm{Aut}(X')$ commuting with F_i' such that $\phi \circ H' = H \circ \phi$. It follows that $H' = \sigma_{X'}^{k}$ and $H = \sigma_X^{nk}$. $\square$

Problem 5.3.13. Does $k(X) = 2$ hold for all infinite *transitive* sofic shifts?

This would follow from a positive answer to Problem 5.2.22 by a similar application of Lemma 5.3.8 as in Proposition 5.3.10.

It would be interesting to find more sensitive isomorphism invariants of $\mathrm{Aut}(X)$. As one possible invariant related to $k(X)$ we suggest

$$k_2(X) = \min\{|S| \mid S \subseteq \mathrm{Aut}(X) \text{ contains only involutions and } C(S) = \langle\sigma\rangle\}.$$

It is previously known by Theorem 7.16 of [53] that $k_2(\Sigma_4^{\mathbb{Z}}) \in \mathbb{N}$. Some upper bounds for this quantity for general mixing sofic shifts can be given by noting that the automorphisms in Proposition 5.3.10 can be represented as compositions of involutions. However, it might be difficult to recognize an optimal upper bound when it has been found. For example, we do not know the answer to the following.

Problem 5.3.14. Does there exist a mixing sofic X such that $k_2(X) = 2$? Do all nontrivial mixing sofics have this property?

5.3.2 A Nontrue Finitary Version of Ryan's Theorem

Finitary Ryan's theorem can be interpreted as a compactness result saying that, for nontrivial mixing sofic shift X, the group $\mathrm{Aut}(X)$ has a finite subset S such that $C(S) = \langle\sigma\rangle$. One may wonder whether this compactness phenomenon is more general: in Section 7.3 of [53] the question was raised whether for a mixing SFT X and for every $R \subseteq \mathrm{Aut}(X)$ such that $C(R) = \langle\sigma\rangle$ there is a finite subset $S \subseteq R$ such that also $C(S) = \langle\sigma\rangle$. In the same section it was noted that to construct a counterexample it would be sufficient to find a locally finite group $\mathcal{G} \subseteq \mathrm{Aut}(X)$ whose centralizer is generated by σ. We use a different strategy based on Lemma 5.3.8 to construct a counterexample in the case when X is the binary full shift.

For every $n \in \mathbb{N}_+$ we define two automorphisms $P_{n,1}, P_{n,2} : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$ as follows. In any $x \in \Sigma_2^{\mathbb{Z}}$,

- $P_{n,1}$ replaces every occurrence of $001^{2n-1}0$ by $011^{2n-1}0$ and vice versa.
- $P_{n,2}$ replaces every occurrence of $01^{2n-1}10$ by $01^{2n-1}00$ and vice versa.

It is easy to see that these maps are well-defined automorphisms of $\Sigma_2^{\mathbb{Z}}$. The maps $G_n : \Sigma_2^{\mathbb{Z}} \to \Sigma_2^{\mathbb{Z}}$ are defined as the compositions $P_{n,2} \circ P_{n,1}$. We will define a tuple $(\mathcal{G}', 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$, which will turn out to be a diffusive glider automorphism group for $\Sigma_2^{\mathbb{Z}}$. Let $\mathcal{G}' = \langle\{G_n \mid i \in \mathbb{N}_+\}\rangle$ and let $\mathcal{I} = \{(n, \reflectbox{ℓ}) \mid n \in \mathbb{N}_+\} \cup \{(n, \ell) \mid n \in \mathbb{N}_+\}$ be the index set. We define gliders $\boxed{\leftrightarrow}_{n,\ell} = \boxed{\leftarrow}_n = 01^{2n-1}$ and $\boxed{\leftrightarrow}_{n,\reflectbox{ℓ}} = \boxed{\rightarrow}_n = 1^{2n}$ and glider fleet sets

$$\mathrm{GF}_{n,\ell} = {}^{\infty}0(\boxed{\leftarrow}_n 00^*)^* 0^{\infty} \qquad \mathrm{GF}_{n,\reflectbox{ℓ}} = {}^{\infty}0(0^*0\boxed{\rightarrow}_n)^* 0^{\infty}.$$

We define languages

$$L_{n,\ell} = (\boxed{\leftarrow}_n 00^*)^* \qquad L_{n,\reflectbox{ℓ}} = (0^*0\boxed{\rightarrow}_n)^*.$$

For $n \in \mathbb{N}_+$ we let $\mathrm{spd}(n,\ell) = 1$, $\mathrm{spd}(n, \reflectbox{ℓ}) = -1$ and $\varsigma_{(n,\reflectbox{ℓ})} = \varsigma_{(n,\ell)} = G_n$.

Lemma 5.3.15. The tuple $(\mathcal{G}', 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ defined above is a glider automorphism group of $\Sigma_2^{\mathbb{Z}}$, i.e. for $n \in \mathbb{N}_+$

- $\mathrm{GF}_{n,\ell}$ is the set of 0-finite configurations x for which $G_n(x) = \sigma(x)$
- $\mathrm{GF}_{n,\reflectbox{ℓ}}$ is the set of 0-finite configurations x for which $G_n(x) = \sigma^{-1}(x)$.

Proof. We prove the first claim, the proof of the second claim being similar. Assume first that $x \in \mathrm{GF}_{n,\ell}$ and assume that $i \in \mathbb{Z}$ is some position in x where $\boxed{\leftarrow}_n$ occurs. Then

$$\begin{aligned}
&x[i-1, i+2n] = 0\boxed{\leftarrow}_n 0 = 0(01^{2n-1})0 \\
&P_{n,1}(x)[i-1, i+2n] = 0(1^{2n})0 \\
&G_n(x)[i-2, i+2n-1] = P_{n,2}(P_{n,1}(x))[i-2, i+2n-1] \\
&= 00(1^{2n-1}0) = 0\boxed{\leftarrow}_n 0,
\end{aligned}$$

so every glider has been shifted by distance 1 to the left and $G_n(x) = \sigma(x)$.

Assume next that $x \in \Sigma_2^{\mathbb{Z}}$ is 0-finite and $G_n(x) = \sigma(x)$. First of all, x cannot contain an occurrence of the pattern $01^{n'}0$ at any position $i \in \mathbb{Z}$ for any $n' \notin \{2n-1, 2n\}$, because otherwise $x[i, i+n'+1] = G_n(x)[i, i+n'+1] = 01^{n'}0$. Second, if x contains an occurrence of the pattern $01^{2n}0$ at a position $i \in \mathbb{Z}$, then $P_{n,1}(x)[i, i+2n+1] = 001^{2n-1}0$ and $G_n(x)[i+1] = 0$, which contradicts $G_n(x)[i+1] = \sigma(x)[i+1] = 1$. Therefore, every occurrence of 1 in x is part of a segment of exactly $2n-1$ consecutive ones. If it were that $x \notin \mathrm{GF}_{n,\ell}$, then x would contain an occurrence of the pattern $101^{2n-1}0$ at some position i. Then $P_{n,1}(x)[i, i+2n+1] = 101^{2n-1}0$ and $G_n(x)[i+1] = 0$, which contradicts $G_n(x)[i+1] = \sigma(x)[i+1] = 1$. $\square$

Lemma 5.3.16. The tuple $(\mathcal{G}', 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ defined above is a diffusive glider automorphism group of $\Sigma_2^{\mathbb{Z}}$.

Proof. By the previous lemma $\mathcal{G}'$ is a glider automorphism group. For the diffusion property it is sufficient to prove for all 0-finite $x \in \Sigma_2^{\mathbb{Z}}$ and $N \in \mathbb{N}$ the existence of a $G \in \mathcal{G}'$ such that $G(x) \in {}^{\infty}0((\cup_{i\in\mathcal{I}} L_i)0^N)^*0^{\infty}$. To do this we define for every 0-finite $x \in \Sigma_2^{\mathbb{Z}}$ the quantity

$$N_x = \sum_{i=1}^{\infty} \left|\mathrm{occ}_{\ell}(x, 01^i0)\right|,$$

i.e. the total number of consecutive runs of ones in x. We remark that $N_x = N_{G(x)}$ for $G \in \mathcal{G}'$, because this clearly holds for $G \in \{P_{n,1}, P_{n,2} \mid n \in \mathbb{N}_+\}$ and these generate a group containing $\mathcal{G}'$. We prove the diffusion property by induction on N_x. As the base case we choose $x \in \mathrm{GF}_s$ ($s \in \mathcal{I}$), for which the claim is trivial. Assume therefore that $x \notin \mathrm{GF}_s$ for all $s \in \mathcal{I}$ and fix $N \in \mathbb{N}$. If the leftmost occurrence of 1 in x is at position $i \in \mathbb{Z}$, then $x[i-1, \infty]$ has the prefix $01^{2n-1}0$ or $01^{2n}0$ for some $n \in \mathbb{N}_+$. We assume without loss of generality that the prefix is of the form $01^{2n-1}0$ (otherwise in the following we replace the map G_n by its inverse G_n^{-1}).

Note that by definition G_n treats words of the form $01^{2n-1}0$ and $01^{2n}0$ in all 0-finite $y \in \Sigma_2^{\mathbb{Z}}$ as gliders which rebound from words of the form $01^{2n'-1}0$ and $01^{2n'}0$ ($n' \neq n$) that remain stationary under the action of G_n as in Figure 5.3 of Subsection 5.1.2. For every $t \in \mathbb{N}$ there is a maximal $i_t \in \mathbb{Z}$ such that $G_n^t(x)[-\infty, i_t] \in {}^{\infty}0(\boxed{\leftarrow}_n 00^*)^*$, so fix $t' \in \mathbb{N}$ such that $G_n^{t'}(x)[-\infty, i_{t'}]$ contains a maximal number of occurrences of $\boxed{\leftarrow}_n$. It is easy to see that also every $t \geq t'$ has this property. Similarly, for every $t \in \mathbb{N}$ there is a minimal $j_t \in \mathbb{Z}$ such that $G_n^t(x)[j_t, \infty] \in (0^*0\boxed{\rightarrow}_n)^*0^{\infty}$, so fix $t \geq t'$ such that $G_n^t[j_t, \infty] \in (0^*0\boxed{\rightarrow}_n)^*0^{\infty}$ contains a maximal number of occurrences of $\boxed{\rightarrow}_n$. If $j_t \leq i_t$, this indicates that $G_n^t(x)$ is of the form $G_n^t(x) \in {}^{\infty}0(0^*0\boxed{\leftarrow}_n)^*(0^*0\boxed{\rightarrow}_n)^*0^{\infty}$ and therefore

$G_n^T(x) \in {}^\infty 0(0^*0\boxed{\leftarrow}_n)^*0^N(0^*0\boxed{\rightarrow}_n)^*0^\infty$ for sufficiently large $T \in \mathbb{N}$, proving our claim. Let us therefore assume in the following that $i_t < j_t$.

Let $y = G_n^t(x)$ and $y = y_1 \otimes_{i_t+1} y_2 \otimes_{j_t} y_3$, where y_1 (resp. y_2 or y_3) agrees with y on the interval $(-\infty, i_t]$ (resp. on the interval (i_t, j_t) or $[j_t, \infty)$) and contains zeroes at all other positions. By the choice of t, i_t, and j_t it follows that

$$G_n^T(y) = \sigma^T(y_1) \otimes_{i_t+1} G_n^T(y_2) \otimes_{j_t} \sigma^{-T}(y_3)$$

and $\mathrm{supp}(G_n^T(y_2)) \subseteq (i_t, j_t)$ for every $T \in \mathbb{N}$, where we denote $\mathrm{supp}(x) = \{i \in \mathbb{Z} \mid x[i] \neq 0\}$ for $x \in \Sigma_2^{\mathbb{Z}}$. Since $N_x = N_{G_n^T(y)} > N_{G_n^T(y_2)}$, it follows from the induction assumption that for every $T \in \mathbb{N}$ there is $G_T \in \mathrm{Aut}(\Sigma_2^{\mathbb{Z}})$ such that

$$G_T(G_n^T(y_2)) \in {}^\infty 0((\cup_{i \in S} L_i)0^N)^*0^\infty.$$

Furthermore all G_T can be chosen so that they are all radius-r automorphisms for some uniform $r \in \mathbb{N}_+$, since there are only finitely many different configurations $G_n^T(y_2)$. Fix therefore $T = 2r + N$. Note also that $G(\mathrm{GF}_{n,\reflectbox{ℓ}} \cup \mathrm{GF}_{n,\ell}) = \mathrm{GF}_{n,\reflectbox{ℓ}} \cup \mathrm{GF}_{n,\ell}$ for $G \in \mathcal{G}'$, because this clearly holds for $G \in \{P_{n',1}, P_{n',2} \mid n' \in \mathbb{N}_+\}$. We see that

$$\begin{aligned} &G_T(G_n^T(y)) = G_T(\sigma^T(y_1)) \otimes_{i_t+1-r} G_T(G_n^T(y_2)) \otimes_{j_t+r} G_T(\sigma^{-T}(y_3)) \\ &\in {}^\infty 0(L_{n,\ell} \cup L_{n,\reflectbox{ℓ}})0^N((\cup_{i \in S} L_i)0^N)^*0^N(L_{n,\reflectbox{ℓ}} \cup L_{n,\ell})0^\infty, \end{aligned}$$

which proves our induction step. □

We construct the group $\mathcal{G}$ generated by $\mathcal{G}'$ and all automorphisms $F_{n,m} = F_{n,m,2} \circ F_{n,m,1}$ for $n, m \in \mathbb{N}_+$ defined as follows. In any $x \in \Sigma_2^{\mathbb{Z}}$,

- $F_{n,m,1}$ replaces every occurrence of $0\boxed{\rightarrow}_n000\boxed{\leftarrow}_m0$ by $0\boxed{\rightarrow}_n00\boxed{\leftarrow}_m00$ and vice versa

- $F_{n,m,2}$ replaces every occurrence of $0\boxed{\rightarrow}_n00\boxed{\leftarrow}_m0$ by $00\boxed{\rightarrow}_n0\boxed{\leftarrow}_m0$ and vice versa.

It is easy to see that these maps are well-defined automorphisms of $\Sigma_2^{\mathbb{Z}}$. Similarly to Example 5.3.9, the map $F_{n,m}$ has two important properties. First, it replaces any occurrence of $0\boxed{\rightarrow}_n000\boxed{\leftarrow}_m0$ by $00\boxed{\rightarrow}_n0\boxed{\leftarrow}_m00$. Second, if $x \in \Sigma_2^{\mathbb{Z}}$ is a configuration containing only gliders $\boxed{\leftarrow}_m$ and $\boxed{\rightarrow}_n$ separated by words from 0^+ and if every occurrence of $\boxed{\leftarrow}_m$ is sufficiently far from every occurrence of $\boxed{\rightarrow}_n$, then $F_{n,m}(x) = x$.

The following two propositions conclude our current example.

Proposition 5.3.17. $C(\mathcal{G}) = \langle \sigma \rangle$

Proof. Since $\mathcal{G}' \subseteq \mathcal{G}$, by the previous lemma $(\mathcal{G}, 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ is also a diffusive glider automorphism group of $\Sigma_2^{\mathbb{Z}}$. We want to use Lemma 5.3.8 to show that $C(\mathcal{G}) \cap \mathrm{Aut}(\Sigma_2^{\mathbb{Z}}, 0) = \langle\sigma\rangle$. The bipartite graph $\mathcal{B}$ in the statement of the lemma has in this case the set of vertices $\mathcal{I}$ with the partition $\mathcal{I}_1 = \{(n, \reflectbox{ℓ}) \mid n \in \mathbb{N}\}$ and $\mathcal{I}_2 = \{(n, \ell) \mid n \in \mathbb{N}\}$, so it suffices to show that there is an edge between $(n, \reflectbox{$\ell$})$ and (k, ℓ) for any fixed $n, k \in \mathbb{N}_+$.

Using the same notation as in the statement of Lemma 5.3.8, let $d = e = 1$ and $(N_m)_{m\in\mathbb{N}}$ with $N_m = 2m + 3$. Let $G_{n,k} = G_n$ if $n = k$, $G_{n,k} = G_n \circ G_k$ if $n \neq k$ and let $(G'_m)_{m\in\mathbb{N}}$ with $G'_m = G_{n,k}^{-(m+1)} \circ F_{n,k} \circ G_{n,k}^m$. Let $x\boxed{\rightarrow}_n \in {}^{\infty}0L_{n,\reflectbox{ℓ}}$ and $\boxed{\leftarrow}_k y \in L_{k,\ell}0^{\infty}$ be arbitrary. Fix some $m \in \mathbb{N}$. It is clear that $x\boxed{\rightarrow}_n.0^{N_m}\boxed{\leftarrow}_k y \in \Sigma_2^{\mathbb{Z}}$ and it is easy to verify that

- $G'_m(x\boxed{\rightarrow}_n.0^N\boxed{\leftarrow}_k y) = x\boxed{\rightarrow}_n 0.0^N 0\boxed{\leftarrow}_k y$ for $N > N_m$
- $G'_m(x\boxed{\rightarrow}_n.0^{N_m}\boxed{\leftarrow}_k y) = x0\boxed{\rightarrow}_n.0^{N_m}\boxed{\leftarrow}_k 0y$.

It follows that there is an edge between $(n, \reflectbox{$\ell$})$ and $(k, \reflectbox{$\ell$})$ and therefore $C(\mathcal{G}) \cap \mathrm{Aut}(\Sigma_2^{\mathbb{Z}}, 0) = \langle\sigma\rangle$.

Now let $H \in C(\mathcal{G})$ be arbitrary. Let us show that $H \in \mathrm{Aut}(\Sigma_2^{\mathbb{Z}}, 0)$. Namely, if it were that $H(0^{\mathbb{Z}}) = 1^{\mathbb{Z}}$, consider $x = {}^{\infty}0.\boxed{\leftarrow}_1 0^{\infty}$ with the glider $\boxed{\leftarrow}_1 = 01$ at the origin and note that $H(x)[i] = 0$ for some $i \in \mathbb{Z}$ and $H(x)[-\infty, j] = {}^{\infty}1$ for some $j \in \mathbb{N}_+$. Then $G_1^t(H(x))[-\infty, j] = {}^{\infty}1$ for every $t \in \mathbb{Z}$ but $H(G_1^{i-j}(x))[j] = H(\sigma^{i-j}(x))[j] = H(x)[i] = 0 \neq 1$, contradicting the commutativity of H and G_1. Thus $H \in \mathrm{Aut}(\Sigma_2^{\mathbb{Z}}, 0)$.

We have shown that $H \in C(\mathcal{G}) \cap \mathrm{Aut}(\Sigma_2^{\mathbb{Z}}, 0) = \langle\sigma\rangle$, so we are done. □

Proposition 5.3.18. If $S \subset \mathcal{G}$ is finite, then $C(S) \supsetneq \langle\sigma\rangle$.

Proof. Fix some finite $S \subseteq \mathcal{G}$. It is a simple observation that for every $F \in S$ there is n_F such that F does not change occurrences of the words $u_n = 01^{n+1}00^n01^{n+1}0$ and $v_n = 01^{n+1}01^n01^{n+1}0$ in any configurations for $n \geq n_F$. Let $n = \max_{F\in S}\{n_F\}$ and let $H \in \mathrm{Aut}(\Sigma_2^{\mathbb{Z}})$ be the automorphism that replaces every occurrence of u_n by v_n (and vice versa) in any configuration $x \in \Sigma_2^{\mathbb{Z}}$. Now it is evident that $H \in C(S)$ even though $H \notin \langle\sigma\rangle$. □

5.4 Restrictions to Constructing Glider Automata

5.4.1 Example: The Choice of 0 in Mixing Sofic Shifts

In Section 5.2 we constructed glider automata on an arbitrary mixing sofic shift X that can diffuse any $\mathbf{0}$-finite configuration into two glider fleets. In other words, the diffusion is guaranteed against the background of the periodic configuration $\mathbf{0}^{\mathbb{Z}}$, but in the construction we required that the word $\mathbf{0}$ satisfies the assumptions of Lemma 5.2.11. One may then ask whether all of these assumptions are necessary. In particular, if we have a subshift

$X \in A^{\mathbb{Z}}$ and a symbol $0 \in A$ such that $0^{\mathbb{Z}} \in X$, it would feel the most natural to consider finiteness with respect to this 1-periodic configuration and ask whether there exists a reversible CA that can diffuse every 0-finite configuration. We show by an example that sometimes this cannot be done.

In this subsection we consider the mixing sofic shift $X \subseteq \{0, 1, a, b, \downarrow, \uparrow\}^{\mathbb{Z}}$ whose language $L(X)$ consists of all the factors of words in $L = (L_0 0^* L_1 0^*)^*$, where

$$L_0 = 1(ab)^*\uparrow(ab)^*\downarrow(ab)^*1 \cup 1(ab)^*\downarrow(ab)^*\uparrow(ab)^*1$$
$$L_1 = 1(ab)^*\downarrow(ab)^*\downarrow(ab)^*1 \cup 1(ab)^*\uparrow(ab)^*\uparrow(ab)^*1.$$

The intuition is that words $w_0 \in L_0$ encode the digit zero (opposing arrows in w_0 negate each other), words $w_1 \in L_1$ encode the digit one (arrows in the same direction in w_1 amplify each other) and in configurations of X consecutive encodings of the same digit cannot occur.

First let us note that $F(0^{\mathbb{Z}}) = 0^{\mathbb{Z}}$ and $F(\mathcal{O}((ab)^{\mathbb{Z}})) = \mathcal{O}((ab)^{\mathbb{Z}})$ for every $F \in \mathrm{Aut}(X)$, because $0^{\mathbb{Z}}$ (resp. $(ab)^{\mathbb{Z}}$) are the only configurations (up to shift) of least period 1 (resp. 2) in X. Throughout this subsection let $e_\ell = {}^\infty 0.1(ab)^\infty$ and $e_{\reflectbox{$\ell$}} = {}^\infty(ab)1.0^\infty$.

Lemma 5.4.1. If $F \in \mathrm{Aut}(X)$, then $F(e_\ell) = \sigma^i(e_\ell)$ and $F(e_{\reflectbox{$\ell$}}) = \sigma^j(e_{\reflectbox{ℓ}})$ for some $i, j \in \mathbb{Z}$.

Proof. Let F be a radius-r reversible CA whose inverse also has radius r. We may assume without loss of generality (by composing F with a suitable shift if necessary) that the rightmost occurrence of 1 in $F(e_\ell)$ is at position 0. We first claim that $F(e_\ell)$ does not contain any occurrence of words from $L_0 \cup L_1$ (equivalently: $F(e_\ell)[-\infty, -1] = {}^\infty 0$). Otherwise assume without loss of generality that the leftmost such occurrence is from L_0. Let $x = {}^\infty 01\uparrow\downarrow 10^{3r+1}.0^\infty$ (i.e. x contains an occurrence of a word from L_0). Its inverse image $F^{-1}(x)$ belongs to X and thus also the gluing $F^{-1}(x) \otimes e_\ell$ belongs to X because the right infinite word $1(ab)^\infty$ in e_ℓ does not give additional constraints for the left side of the sequence. But then the configuration $F(F^{-1}(x) \otimes e_\ell)$ contains two consecutive occurrences of words from L_0, contradicting the definition of X.

Now to prove that $F(e_\ell) = e_\ell$ it remains to show that $F(e_\ell)$ cannot contain any arrows, so we assume to the contrary that $F(e_\ell)$ contains one or two arrows. The possibility that $F(e_\ell)$ contains two arrows yields a contradiction by the same argument as in the previous paragraph (e.g. if $F(e_\ell)$ contains two opposing arrows, then glue $F^{-1}(x) \otimes e_\ell$, in which case $F(F^{-1}(x) \otimes e_\ell)$ contains two consecutive encodings of the digit 0), so let us assume that $F(e_\ell)$ contains a single arrow (whose distance from the single 1 in $F(e_\ell)$ is at most r). Let $e'_\ell = {}^\infty 0.1(ab)^{2r+1}\uparrow(ab)^\infty$. Since F is reversible, it follows that $F(e_\ell) \neq F(e'_\ell)$ and in particular $F(e'_\ell)$ contains two arrows. Now we can use the same argument as above to show that this is not possible, so we conclude that $F(e_\ell) = e_\ell$.

By symmetry $F(e_{\reflectbox{$\ell$}}) = \sigma^j(e_{\reflectbox{ℓ}})$ for some $j \in \mathbb{Z}$. $\square$

For now, if F, i, j are as in the previous lemma, we say that the *intrinsic left (resp. right) shift* of F is equal to i (resp. equal to j). In the following let $x_\uparrow = {}^\infty(ab).\uparrow(ab)^\infty$ and $x_\downarrow = {}^\infty(ab).\downarrow(ab)^\infty$.

Lemma 5.4.2. If $F \in \mathrm{Aut}(X)$ has intrinsic left shift i (resp. intrinsic right shift i), then $F(x_\uparrow) \in \sigma^i(\{x_\uparrow, x_\downarrow\})$ and $F(x_\downarrow) \in \sigma^i(\{x_\downarrow, x_\uparrow\})$. In particular the intrinsic right and left shift are equal.

Proof. Let F be a radius-r reversible CA whose inverse also has radius r and assume without loss of generality (by composing F with a suitable shift if necessary) that the intrinsic left shift is $i = 0$, the case of the intrinsic right shift $i = 0$ being symmetric. We prove the claim for $F(x_\uparrow)$, the other case being symmetric. We first claim that $F(x_\uparrow) \in \mathcal{O}(x_\uparrow) \cup \mathcal{O}(x_\downarrow)$. Otherwise $F(x_\uparrow)$ contains at least two occurrences of arrows or at least one occurrence of 1. Denoting $y = {}^\infty 0.1(ab)^{2r+1}\uparrow(ab)^\infty$, in both cases $F(y)[-\infty, 2r+1] = {}^\infty 0.1(ab)^r$ by the previous lemma, and going further to the right in $F(y)$ there must be two occurrences of arrows after which there may be an occurrence of 1. We will derive a contradiction in the case that these arrows point in opposing directions, after which it will be clear that a similar argument yields a contradiction the case that the arrows point in the same direction. Let $x = {}^\infty 01\uparrow\downarrow 10^{3r+1}.0^\infty$ (i.e. x contains an occurrence of a word from L_0). The gluing $F^{-1}(x) \otimes y$ belongs to X because the right infinite word $1(ab)^{2r+1}\uparrow(ab)^\infty$ in y does not give additional constraints for the left side of the sequence. But then the configuration $F(F^{-1}(x) \otimes y) = x \otimes F(y)$ contradicts the definition of X.

Now we prove that $F(x_\uparrow) \in \{x_\uparrow, x_\downarrow\}$. Otherwise it holds that $F(x_\uparrow) \in \{\sigma^k(x_\uparrow), \sigma^k(x_\downarrow)\}$ for $k \neq 0$ and we may assume without loss of generality that $0 < k \leq r$ (by considering instead the CA F^{-1} if necessary) and that $F(x_\uparrow) = \sigma^k(x_\uparrow)$ (by composing F with the CA that only flips the direction of every arrow if necessary). Consider the point $x = {}^\infty 0.1(ab)^{2r+1}\uparrow(ab)^\infty$. None of the configurations $F^t(x)$ ($t \in \mathbb{N}$) contain an occurrence of a word from $L_0 \cup L_1$ by the same argument as in the previous paragraph and as in the proof of the previous lemma. Similarly none of the $F^t(x)$ contain two arrows and the unique arrow in $F^t(x)$ points to the direction $\uparrow$. Since $F(x_\uparrow) = \sigma^k(x_\uparrow)$, it follows that for $t > 0$ the distance between 1 and $\uparrow$ in $F^t(x)$ is strictly smaller than in x and in particular $F^t(x) \notin \mathcal{O}(x)$. However, from $F(x_\uparrow) = \sigma^k(x_\uparrow)$ it also follows that in each $F^t(x)$ the distance between 1 and $\uparrow$ is bounded, so $F^{t'}(x) = \sigma^m(F^{2t'}(x))$ for some $t' \in \mathbb{N}_+$, $m \in \mathbb{Z}$. Therefore $\sigma^m(F^{2t'}(x))$ has two distinct preimages under the map $\sigma^m \circ F^{t'}$

(they are $F^{t'}(x)$ and $\sigma^{-m}(x)$, for distinctness recall that $F^t(x) \notin \mathcal{O}(x)$ for $t \in \mathbb{N}_+$), which contradicts the reversibility of F. $\square$

In the following we say that the *intrinsic shift* of $F \in \mathrm{Aut}(X)$ is equal to i if i is its intrinsic left (or equivalently right) shift. Next we will conclude that for any $F \in \mathrm{Aut}(X)$ there are 0-finite configurations with long contiguous segments of non-0 symbols on which F cannot do anything nontrivial. In fact, this holds for every finitely generated subgroup of $\mathrm{Aut}(X)$.

Proposition 5.4.3. For all $n \in \mathbb{N}$ let $x_n = {}^{\infty}0.1(ab)^n{\uparrow}(ab)^n{\uparrow}(ab)^n 10^{\infty}$, $y_n = {}^{\infty}0.1(ab)^n{\downarrow}(ab)^n{\downarrow}(ab)^n 10^{\infty}$ and $Z_n = \mathcal{O}(\{x_n\}) \cup \mathcal{O}(\{y_n\})$. For every finitely generated $\mathcal{G}$ there is $N \in \mathbb{N}$ such that $F(Z_n) = Z_n$ for all $F \in \mathcal{G}$ and $n \geq N$.

Proof. Let $\{F_1, \dots, F_k\} \subseteq \mathrm{Aut}(X)$ be a finite set that generates $\mathcal{G}$. Since the statement of the proposition concerns the shift-invariant sets Z_n, we may assume without loss of generality (by composing all the F_i by suitable powers of the shift if necessary) that the intrinsic shift of every F_i is equal to 0. Fix a number $r \in \mathbb{N}$ such that all the F_i are radius-r CA whose inverses are also radius-r CA. To prove the claim it is sufficient to show that $F_i(\{x_n, y_n\}) = \{x_n, y_n\}$ for every $n \geq 2r+1$ and for every $1 \leq i \leq k$. But this conclusion directly follows from the two previous lemmas. $\square$

5.4.2 Example: Shifts with Specification

In this subsection we address Remark 5.2.21.

Definition 5.4.4. We say that a subshift X is a *shift with specification* (with transition length $n \in \mathbb{N}$) if for every $u, v \in L(X)$ there is a $w \in L^n(X)$ such that $uwv \in L(X)$.

All shifts with specification are synchronizing [3].

For $S \subseteq \mathbb{N}$, we define the S-gap shift $X_S \subseteq \Sigma_2^{\mathbb{Z}}$ as the subshift determined by the collection of forbidden patterns $\{01^n0 \mid n \notin S\}$ (when S is finite, we also forbid 1^n for some n larger than any element of S: in our considerations the finite case will not come up). We may equate S with its characteristic sequence and we write $S(i) = 1$ if $i \in S$ and $S(i) = 0$ if $i \notin S$ (for $i \in \mathbb{N}$).

By Example 3.4 of [29] the subshift X_S has the specification property if and only if the sequence $S \in \Sigma_2^{\mathbb{N}}$ does not contain arbitrarily long runs of zeroes between two ones and $\gcd\{n+1 \mid n \in S\} = 1$. We prove our lemmas for S-gap shifts such that $0 \in S$ and the sequence S is not eventually periodic: this class of subshifts contains many shifts with specification.

Lemma 5.4.5. If $0 \in S$ and S is not eventually periodic, then any $F \in \mathrm{Aut}(X_S)$ has $0^{\mathbb{Z}}$ and $1^{\mathbb{Z}}$ as fixed points.

Proof. Assume to the contrary that $F(0^{\mathbb{Z}}) = 1^{\mathbb{Z}}$ and $F(1^{\mathbb{Z}}) = 0^{\mathbb{Z}}$ and consider the sequence of points $x_n = {}^{\infty}10^n1^{\infty} \in X_S$ ($n \in \mathbb{N}$). Clearly the configurations $F(x_n)$ contain as factors the words 01^n0 for all sufficiently large n. But then $\mathbb{N} \setminus S$ would have to be finite, contradicting the assumption that S is not eventually periodic. $\square$

For the rest of this section let $X_{S,\ell} = \{x \in X_S \mid x[0,\infty] = 01^{\infty}\}$ and $X_{S,\reflectbox{$\ell$}} = \{x \in X_S \mid x[-\infty,0] = {}^{\infty}10\}$. These sets are non-empty whenever S is infinite.

Lemma 5.4.6. Assume that $0 \in S$ and S is not eventually periodic. For every $F \in \mathrm{Aut}(X_S)$ there exists $i \in \mathbb{Z}$ such that $F(X_{S,\ell}) \subseteq \sigma^i(X_{S,\ell})$ and $F(X_{S,\reflectbox{$\ell$}}) \subseteq \sigma^i(X_{S,\reflectbox{ℓ}})$.

Proof. Let $x_{\reflectbox{$\ell$}} \in X_{S,\reflectbox{$\ell$}}$ be arbitrary. Without loss of generality (by composing F with a suitable power of the shift if necessary) we may assume that $F(x_{\reflectbox{$\ell$}}) \in X_{S,\reflectbox{ℓ}}$. We will show that $F(X_{S,\ell}) \subseteq X_{S,\ell}$. Let us therefore assume to the contrary and without loss of generality (by considering F^{-1} instead of F if necessary) that there exists $x_\ell \in X_{S,\ell}$ such that $F(x_\ell) \in \sigma^i(X_{S,\ell})$ for some $i > 0$. Since S is not eventually periodic, it follows that there are arbitrarily large $j \in \mathbb{N}$ such that $S(j) = 1$ and $S(j+i) = 0$. This is a contradiction, because for sufficiently large such j it holds that $x = x_\ell[-\infty,1]01^j.0x_{\reflectbox{ℓ}}[1,\infty] \in X_S$, but from $F(x_\ell) \in \sigma^i(X_{S,\ell})$ and $F(x_{\reflectbox{$\ell$}}) \in X_{S,\reflectbox{ℓ}}$ it follows that $F(x)$ contains an occurrence of the forbidden pattern $01^{j+i}0$.

Because $F(X_{S,\ell}) \subseteq X_{S,\ell}$, we can use the argument of the previous paragraph to show that $F(X_{S,\reflectbox{$\ell$}}) \subseteq X_{S,\reflectbox{ℓ}}$. $\square$

If F and i are as in the previous lemma, we say that the *intrinsic shift* of F is equal to i. If $i = 0$, we say that F is *shiftless*.

Corollary 5.4.7. Assume that $0 \in S$ and S is not eventually periodic. Let $F \in \mathrm{Aut}(X_S)$ be a shiftless radius-r automorphism and let $f : \Sigma_2^{2r+1} \to \Sigma_2$ be a local rule that defines F. For any word $w \in \Sigma_2^r$ the following hold: $f(w01^r) = f(1^r0w) = 0$, $f(w1^{r+1}) = 1$ and $f(1^{r+1}w) = 1$ (whenever all the words involved are from $L(X_S)$).

Corollary 5.4.8. Assume that $0 \in S$ and S is not eventually periodic. Let $F \in \mathrm{Aut}(X_S)$ be a shiftless radius-r automorphism whose inverse is also a radius-r automorphism. If $x \in X_S$, $i \in \mathbb{Z}$ and $n \geq 2r$, then 01^n0 occurs in x at position i if and only if it occurs in $F(x)$ at position i.

Now we can show that Theorem 5.2.20 does not extend to shifts with specification.

Theorem 5.4.9. Assume that $0 \in S$ and S is not eventually periodic. Then all reversible cellular automata $F : X_S \to X_S$ have an almost equicontinuous direction.

Proof. Assume that F has intrinsic shift i. Then $F' = \sigma^{-i} \circ F$ is shiftless. Let r be a radius for both F' and its inverse and choose an arbitrary $n \in S$ such that $n \geq 2r$. By the previous corollary the word 01^n0 is blocking for F' so by Proposition 2.4.3 F' is almost equicontinuous. Then $-i$ is an almost equicontinuous direction for F. $\square$

Corollary 5.4.8 can also be used to show that Theorem 5.3.11 (Finitary Ryan's theorem) does not extend to shifts with specification.

Theorem 5.4.10. If $0 \in S$ and S is not eventually periodic, then $k(X_S) \notin \mathbb{N}$.

Proof. Assume to the contrary that $R \subseteq \mathrm{Aut}(X_S)$ is a set of cardinality of $n \in \mathbb{N}$ such that $C(R) = \langle \sigma \rangle$. By composing the elements of R by suitable powers of the shift we may assume without loss of generality that all the elements of R are shiftless. Fix a number $r \in \mathbb{N}_+$ such that all elements of R are radius-r automorphisms whose inverses are also radius-r automorphisms.

Let $n_1 < n_2 < n_3 \in S$ be three distinct numbers such that $n_i \geq 2r$. Let $w_i = 1^{n_i}$ and let $H \in \mathrm{Aut}(X_S)$ be the automorphism which given a point $x \in X_S$ replaces every occurrence of the pattern

$$0w_30w_10w_20 \qquad \text{by} \qquad 0w_30w_20w_10$$

and vice versa (it exists by Lemma 5.2.13 with the choice $u = 0$). In light of Corollary 5.4.8 it is evident that the elements of R cannot remove or add occurrences of the patterns defined above, so H commutes with every element of R, a contradiction. $\square$

Theorem 5.4.11. If $0 \in S$ and S is not eventually periodic, then $k(X_S) = \infty$.

Proof. By the previous theorem it is sufficient to show that $C(\mathrm{Aut}(X_S)) = \langle \sigma \rangle$. Let therefore $F \in \mathrm{Aut}(X_S) \setminus \langle \sigma \rangle$ be an arbitrary radius-r automorphism. We will show that $F \notin C(\mathrm{Aut}(X_S))$ and we may assume without loss of generality that F is shiftless (by composing F with a suitable shift if necessary). For $w \in \Sigma_2^*$ denote

$$x_w = {}^\infty 10^{2r+1}.w0^{2r+1}1^\infty,$$
$$D = \{x_w \mid w \in \Sigma_2^*, x_w \in X_S\}.$$

Fix $x_w \in D$ such that $F(x_w) \neq x_w$. It exists, because otherwise $F = \mathrm{Id}$ would follow by the denseness of $\mathcal{O}(D)$ in X_S. Fix $n = |w|$ and let $n_1 < n_2 \in S$ be numbers such that $n_i \geq 2r$ and $n_i > n$. Construct the configurations

$$y = {}^{\infty}01^{n_2}0^{2r+1}.w0^{2r+1}1^{n_1}0^{\infty}, \qquad y' = {}^{\infty}01^{n_2}0^{2r+1}.0^{n}0^{2r+1}1^{n_1}0^{\infty}.$$

Since $F(x_w) \neq x_w$, it follows that $F(y) \neq y$. Because F is shiftless and fixes the point $0^{\mathbb{Z}}$, it also follows that $F(y') = y'$ and in particular $F(y) \neq y'$.

Let $G : X_S \to X_S$ be the automorphism that replaces every occurrence of the word

$$01^{n_2}0^{2r+1}w0^{2r+1}1^{n_1}0 \qquad \text{by} \qquad 01^{n_2}0^{2r+1}0^{n}0^{2r+1}1^{n_1}0$$

and vice versa (it exists by Lemma 5.2.13 with the choice $u = 0$). Because $F(y) \notin \{y, y'\}$, we see that $G(F(y)) = F(y)$. It holds that $F(G(y)) \neq F(y) = G(F(y))$, so $F \notin C(\mathrm{Aut}(X_S))$.

□

We conclude this subsection with some speculations. We guess that whenever X is a transitive subshift for which $\mathrm{Aut}(X)$ is "large" as an abstract group, then $k(X) < \infty$ implies that $\mathrm{Aut}(X)$ contains a reversible CA without almost equicontinuous directions. This would be interesting because it would connect a group theoretical property of $\mathrm{Aut}(X)$ to the possible CA dynamics on the subshift X.

The group $\mathrm{Aut}(X)$ is large at least when X is an infinite synchronizing subshift in the sense that it contains an isomorphic copy of the free product of all finite groups [17]. If X is a nontrivial mixing sofic shift, then by Theorems 5.2.20 and 5.3.11 $\mathrm{Aut}(X)$ contains a CA without almost equicontinuous directions and $k(X) = 2$. On the other hand, in this subsection we saw examples of subshifts X with the specification property such that every $F \in \mathrm{Aut}(X)$ has a direction that admits blocking words and we used the existence of blocking words to prove that $k(X) = \infty$.

The assumption of largeness of $\mathrm{Aut}(X)$ is necessary. By [17] for any finite group $\mathcal{G}$ there is a so-called coded subshift X such that $\mathrm{Aut}(X) \simeq \mathbb{Z} \oplus \mathcal{G}$, where the part $\mathbb{Z}$ corresponds to the shift maps. Then $k(X) = 0$ whenever $C_{\mathcal{G}}(\mathcal{G}) = \{1_{\mathcal{G}}\}$ but every element of $\mathrm{Aut}(X)$ has an almost equicontinuous direction.

Problem 5.4.12. Is $k(X) \notin \mathbb{N}$ for every infinite synchronizing subshift X such that every $F \in \mathrm{Aut}(X)$ admits an almost equicontinuous direction?

We note that there are synchronizing non-sofic subshifts that admit CA with only sensitive directions. For example, whenever X is synchronizing and non-sofic, then so is also $Y = X \times X$ and the CA $F : Y \to Y$ defined by $F(x_1, x_2) = (\sigma(x_1), \sigma^{-1}(x_2))$ for $x_1, x_2 \in X$ has only sensitive directions.

In the light of examples such as this, it is not clear what kind of an answer one should expect to the following problem.

Problem 5.4.13. Characterize the transitive non-sofic subshifts that admit reversible CA with only sensitive directions.

We guess that $k(Y) = \infty$ at least when $Y = X_S \times X_S$ for some synchronizing non-sofic S-gap shift X_S, which would mean that the existence of reversible CA with only sensitive directions is not sufficient to prove a finitary Ryan's theorem for general synchronizing shifts.

Problem 5.4.14. Is $k(X) \notin \mathbb{N}$ for every non-sofic synchronizing subshift X?

We also ask whether the existence of a reversible CA $F : X \to X$ with only sensitive directions on a subshift X has a simple dynamical characterization based on X or a simple combinatorial characterization based on the language $L(X)$ or the syntactic monoid S_X.

5.5 Finitary Ryan's Theorem for $\mathrm{End}(\Sigma_n^{\mathbb{Z}})$

We conclude this chapter by proving an optimal endomorphism version of finitary Ryan's theorem for full shifts. The following is essentially Definition 4.2.33 of [52] and it is the endomorphism version of Definition 5.3.1.

Definition 5.5.1. For a subshift X, let $m(X) \in \mathbb{N} \cup \{\infty, \perp\}$ be the minimal cardinality of a set $S \subseteq \mathrm{End}(X)$ such that $C_{\mathrm{End}(X)}(S) = \langle \sigma \rangle$ if such a set S exists, and $m(X) = \perp$ otherwise.

Salo proves the following theorem.

Theorem 5.5.2. [52, Theorem 4.2.32] If $n \geq 3$ then $m(\Sigma_n^{\mathbb{Z}}) \leq 3$.

To be more precise, in [52] it is shown that the set $S \subseteq \mathrm{End}(\Sigma_n^{\mathbb{Z}})$ containing all (not necessarily reversible) symbol maps on Σ_n has a centralizer consisting of only shift maps. The theorem as given here follows by noting that there is a set $S' = \{F_1, F_2, F_3\} \subseteq S$ of cardinality 3 which generates S as a monoid, where F_1 is the cyclic permutation $(01 \dots (n-1))$, F_2 is the transposition (01) and F_3 maps the symbol 1 to 0 and every other symbol to itself.

Later we will improve Theorem 5.5.2 by extending it to all full shifts and by finding the correct value of $m(\Sigma_n^{\mathbb{Z}})$ instead of just an upper bound. First we recall some basics on homomorphic cellular automata.

Definition 5.5.3. Let $(A, +)$ be a finite abelian group. If $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a CA which is a group homomorphism when $A^{\mathbb{Z}}$ is interpreted as the direct product group of $(A, +)$, we say that F is a *homomorphic* CA.

The following two lemmas are well known and their proofs are found for example in [52].

Lemma 5.5.4. [52, Lemma 4.1.7] Let $(A, +)$ be a finite abelian group and $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a homomorphic CA defined by a local rule $f : A^{d+1} \to A$. Then there are group homomorphisms $f_i : A \to A$ such that $f(a_1, \ldots, a_{d+1}) = \sum_{i=1}^{d+1} f_i(a_i)$ for all $a_i \in A$.

Lemma 5.5.5. [52, Lemma 4.1.8] Let $(\Sigma_n, +)$ be a cyclic group of cardinality n. If $F : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ is a homomorphic CA defined by a local rule $F : \Sigma_n^{d+1} \to \Sigma_n$, then there are $k_i \in \mathbb{N}$ such that $f(a_1, \ldots, a_{d+1}) = \sum_{i=1}^{d+1} k_i a_i$ for all $a_i \in \Sigma_n$.

Proof. This follows from the previous lemma, because every group homomorphism $f_i : \Sigma_n \to \Sigma_n$ on the cyclic group Σ_n is determined by how it maps the generator $1 \in \Sigma_n$ and therefore it is of the form $f_i(a) = k_i a$ ($k_i \in \mathbb{N}$, $a \in \Sigma_n$). □

Definition 5.5.6. Let $(A, +)$ be a finite abelian group. We say that a CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is *homomorphic plus constant* (homomorphic+C) if there exist a homomorphic CA $G : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ and a constant configuration $e \in A^{\mathbb{Z}}$ such that $F(x) = G(x) + e$ for every $x \in A^{\mathbb{Z}}$.

Definition 5.5.7. A CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is *bipermutive* if it can be defined by a local rule $f : A^{d+1} \to A$ such that $d \geq 1$ and for every $w \in A^d$ it holds that $f(a, w) \neq f(b, w)$ and $f(w, a) \neq f(w, b)$ whenever $a, b \in A$ are distinct (i.e. F is both left and right permutive).

The following theorem was originally proved in [7] for those bipermutive homomorphic+C CA that can be defined by a local rule with memory 0 and anticipation 1.

Theorem 5.5.8. [52, Theorem 4.3.24] Let $(A, +)$ be a finite abelian group and let $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a bipermutive homomorphic+C CA. If $G : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a CA that commutes with F, then G is homomorphic+C.

We are now ready to give the improvement of Theorem 5.5.2.

Theorem 5.5.9. $m(\Sigma_n^{\mathbb{Z}}) = 2$ for all $n \geq 2$.

Proof. We consider $(\Sigma_n, +)$ as the cyclic group of n elements. Define a local rule $g : \Sigma_n^3 \to \Sigma_n$ by

$$g(a_{-1}, a_0, a_1) = \begin{cases} 1 \text{ when } (a_{-1}, a_0, a_1) = (0, 1, 0) \text{ and} \\ a_0 + 1 \pmod{n} \text{ otherwise} \end{cases}$$

for all $a_{-1}, a_0, a_1 \in \Sigma_n$ and the corresponding CA function $G : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ by

$$G(x)[i] = g(x[i-1], x[i], x[i+1])$$

for $x \in \Sigma_n^{\mathbb{Z}}$ and $i \in \mathbb{Z}$. Let $F : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ be the bipermutive homomorphic CA defined by $F(x)[i] = x[i] + x[i+1]$ for all $x \in \Sigma_n^{\mathbb{Z}}$, $i \in \mathbb{Z}$. Let $S = \{F, G\}$. We claim that the centralizer of $S \subseteq \mathrm{End}(\Sigma_n^{\mathbb{Z}})$ consists of only shift maps, from which it will follow that $m(\Sigma_n^{\mathbb{Z}}) \leq 2$. Assume therefore to the contrary that $H : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ is a cellular automaton which commutes with F and G but is not a power of σ. The commutativity with F in conjunction with Theorem 5.5.8 implies that H is homomorphic+C. By Lemma 5.5.5 H can be defined by a local rule $h : \Sigma_n^{d+1} \to \Sigma_n$ with d minimal and $h(a_1, \dots, a_{d+1}) = \sum_{i=1}^{d+1} k_i a_i + b$ for some fixed $k_i \in \mathbb{N}$ and $b \in \Sigma_n$. Furthermore, we may assume that $0 \leq k_i < n$, and by the minimality of d it follows that $k_1, k_{d+1} \neq 0$. Denote by m the memory of H.

Assume first that $d \geq 1$ and that H is bipermutive. By assumption G commutes with H, so it follows by Theorem 5.5.8 that G is homomorphic+C. To see that this is not possible, assume that $G = G' + e$, where G' is homomorphic and e is a constant configuration. Let $x_1 = \cdots 000.1000 \cdots$ and $x_2 = \cdots 111.0111 \cdots$ (x_1 and x_2 are constant everywhere except at the origin). Because $x_1 + x_2 = 1^{\mathbb{Z}}$, it follows that $G(x_1 + x_2)$ is a constant configuration. On the other hand,

$$\begin{aligned} &G(x_1 + x_2) = G'(x_1) + G'(x_2) + e = G(x_1) + G(x_2) - e \\ &= 1^{\mathbb{Z}} + \cdots 222.1222 \cdots - c \end{aligned}$$

is not a constant configuration because $\cdots 222.1222 \cdots$ is not constant, a contradiction.

Assume then that $d \geq 1$ and that H is not bipermutive. This is the same as saying that either k_1 or k_{d+1} is divisible by a prime factor of n. Both cases are similar, so assume that k_1 is divisible by a prime factor of n. In fact we will get the contradiction from the weaker assumption that $k_1 \notin \{0, 1\}$ and $d \geq 0$. Let $x = \cdots 000.1000 \cdots$. It follows that

$$G(x)[0, \infty] = 111 \cdots \qquad \text{and} \qquad H(x)[-m, \infty] = (k_1 + b)bbb \cdots .$$

The sequence $H(G(x))[-m, \infty]$ is constant, so $G(H(x))[-m, \infty]$ should also be constant. However, if $b \neq 0$ then

$$G(H(x))[-m, \infty] = (k_1 + b + 1)(b + 1)(b + 1)(b + 1) \cdots$$

and if $b = 0$, then from $k_1 \neq 1$ it follows that $G(H(x))[-m, \infty] = (k_1 + 1)111 \cdots$. These are not constant sequences because $k_1 \neq 0$.

Assume then that $d = 0$, i.e. the local rule of H is of the form $h(a) = k_1 a + b$ for fixed $k_1 \in \mathbb{N}$, $b \in \Sigma_n$. Without loss of generality (by composing

H with a suitable shift if necessary) we may assume that the memory and anticipation of H are 0. Assume first that $k_1 = 0$, i.e. H is a constant map that maps every configuration to $b^{\mathbb{Z}}$. Then

$$H(G(0^{\mathbb{Z}})) = H(1^{\mathbb{Z}}) = b^{\mathbb{Z}} \neq G(b^{\mathbb{Z}}) = G(H(0^{\mathbb{Z}})),$$

which contradicts the commutativity assumption. The case $k_1 \notin \{0, 1\}$ was shown to be impossible in the previous paragraph, so the case $k_1 = 1$ and $b \neq 0$ remains (the case $k_1 = 1$ and $b = 0$ means that H is the identity map). Let $x = \cdots 000.1000 \cdots$. Then $H(x) = \cdots bbb.(b+1)bbb \cdots$ and $G(H(x)) = \cdots (b+1)(b+1)(b+1).(b+2)(b+1)(b+1)(b+1) \cdots$ is not a constant configuration. On the other hand, $H(G(x)) = H(1^{\mathbb{Z}}) = (b+1)^{\mathbb{Z}}$ is a constant configuration, which contradicts the commutativity assumption.

We now know that $m(\Sigma_n^{\mathbb{Z}}) \leq 2$. Note that $\mathrm{End}(\Sigma_n^{\mathbb{Z}}) \neq \langle \sigma \rangle$, so an argument analogous to that in Theorem 5.3.2 shows that $m(\Sigma_n^{\mathbb{Z}}) < 2$ is not possible and therefore $m(\Sigma_n^{\mathbb{Z}}) = 2$ $\square$

The proof of this result used homomorphic cellular automata and it does not seem to generalize to more general subshifts. We repeat here a question from [52].

Problem 5.5.10. Does $m(X) = 2$ for all mixing SFTs containing at least two constant configurations?

Chapter 6

Summary of Open Problems

We collect here all the open problems presented in the thesis. More context can be found from those parts of the thesis where they first appear.

In Chapter 3 we studied the class of multiplication automata. This is a natural class of cellular automata with complex behavior and they are of interest because many of them eventually generate all finite sequences when initialized on any finite nontrivial configuration. In fact, this class contains essentially the only known universal pattern generators. Conjecturally some of them are also strong universal pattern generators. The following are presented as Problems 3.1.9, 3.1.10 and 3.1.11 in the main text.

Problem. Does there exist a weak universal pattern generator over the binary alphabet Σ_2?

Problem. Do any strong universal pattern generators exist? For example, is the automaton $\Pi_{3/2,6}$ a strong universal pattern generator together with any finite configurations?

Problem. Do any non-reversible universal pattern generators exist?

Wolfram's Rule 30 automaton W_{30} is conjecturally a non-reversible weak universal pattern generator over the alphabet Σ_2. Few rigorous results concerning W_{30} have been proved, even though it can be defined by a simple formula. It would be interesting to know what other properties W_{30} might share with known universal pattern generators. By Corollary 3.4.19 we know that the weak universal pattern generator $\Pi_{p/q,pq}$ with coprime $p > q > 1$ is not regular. This motivates problem 3.1.13.

Problem. Is W_{30} regular?

We observed that the only reversible multiplication automaton contained in the kernel of the group homomorphism $\delta : \mathrm{Aut}(\Sigma_n^{\mathbb{Z}}) \to \mathbb{R}_{>0}$ defined in [31] is the identity map. In particular none of the known weak universal pattern generators are in the kernel of δ. It is probably not reasonable to conjecture that this holds more generally, but we still present Problem 3.2.6.

Problem. Does the kernel of $\delta : \mathrm{Aut}(\Sigma_n^{\mathbb{Z}}) \to \mathbb{R}_{>0}$ contain a weak universal pattern generator for any $n \geq 2$?

In Theorem 3.6.6 we saw that the multiplication automata $\Pi_{p/q,pq}$ with $p > q > 1$ are strongly mixing with respect to the uniform measure. The proof uses a kind of a weak permutivity property of $\Pi_{p/q,pq}$. In Problem 3.6.9 we ask what is a natural generalization of this result.

Problem. How should one define the class $\mathcal{C}_{\mathrm{wp}} \subseteq \mathrm{End}(A^{\mathbb{Z}})$ of *weak permutive* cellular automata? We want a natural definition such that $\mathcal{C}_{\mathrm{wp}}$ contains all permutive cellular automata as a proper subset and that the elements of $\mathcal{C}_{\mathrm{wp}}$ are strongly mixing with a proof analogous to the proof of Theorem 3.6.6.

Starting from Chapter 4 we turn from considerations of naturally occurring cellular automata to more elaborate constructions. In Chapter 4 we proved that the Lyapunov exponents of reversible cellular automata on full shifts cannot be computed to arbitrary precision. In Problems 4.2.4, 4.2.5 and 4.2.6 we ask other questions concerning Lyapunov exponents.

Problem. Is there a fixed mixing SFT X such that the Lyapunov exponents of a given reversible CA $F : X \to X$ cannot be computed to arbitrary precision? Can we choose here $X = \Sigma_2^{\mathbb{Z}}$? Can X be any mixing SFT?

Problem. Is it decidable whether the equality $\lambda^+(F) + \lambda^-(F) = 0$ holds for a given reversible cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$?

Problem. Does there exist a single cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ such that $\lambda^+(F)$ is an uncomputable number?

In Chapter 5 we constructed diffusive glider CA on all nontrivial mixing sofic shifts. This construction shows that all nontrivial mixing sofic shifts have reversible cellular automata without almost equicontinuous directions. In Problems 5.2.22 and 5.4.13 we ask how much is it possible to extend these results in the class of transitive subshifts. We are very confident that the first question has a positive answer.

Problem. Is it possible to generalize the construction of a diffusive glider CA presented in Section 5.2 to the class of all infinite transitive sofic shifts?

Problem. Characterize the transitive non-sofic subshifts that admit reversible CA with only sensitive directions.

To each subshift X one can associate the quantity $k(X)$ which is the minimal size of a collection of reversible cellular automata whose centralizer in $\mathrm{Aut}(X)$ is equal to $\langle \sigma \rangle$. This quantity is an isomorphism invariant of the group $\mathrm{Aut}(X)$. Using diffusive glider CA we found that $k(X) = 2$ for all nontrivial mixing sofic subshifts. In Problem 5.3.13 we ask whether this result extends to the class of all infinite transitive sofic shifts, once again expecting a positive answer.

Problem. Does $k(X) = 2$ hold for all infinite transitive sofic shifts?

We also define a potentially finer invariant $k_2(X)$, which is the topic of Problem 5.3.14.

Problem. Does there exist a mixing sofic X such that $k_2(X) = 2$? Do all nontrivial mixing sofics have this property?

Because the proof of the equality $k(X) = 2$ uses diffusive glider CA, we ask whether extending this result for more general synchronizing subshifts absolutely requires the existence of such cellular automata. This question is what motivates Problems 5.4.12 and 5.4.14.

Problem. Is $k(X) \notin \mathbb{N}$ for every infinite synchronizing subshift X such that every $F \in \mathrm{Aut}(X)$ admits an almost equicontinuous direction?

Problem. Is $k(X) \notin \mathbb{N}$ for every non-sofic synchronizing subshift X?

To each subshift X one can also associate the quantity $m(X)$, which is an analogue of $k(X)$ for the endomorphism monoid $\mathrm{End}(X)$. Using previously known results on homomorphic cellular automata we proved that $m(\Sigma_n^{\mathbb{Z}}) = 2$ for all $n \geq 2$. Problem 5.5.10 asks whether this result can be generalized.

Problem. Does $m(X) = 2$ for all mixing SFTs containing at least two constant configurations?

Bibliography

[1] Shigeki Akiyama, Christiane Frougny, and Jacques Sakarovitch. Powers of rationals modulo 1 and rational base number systems. *Israel Journal of Mathematics*, 168:53–91, 2008.

[2] Daniel Berend. Multi-invariant sets on compact abelian groups. *Transactions of the American Mathematical Society*, 286(2):505–535, 1984.

[3] Anne Bertrand. Specification, synchronisation, average length. In *International Colloquium on Coding Theory and Applications*, pages 86–95. Springer, 1986.

[4] F. Blanchard, B. Host, and A. Maass. Représentation par automate de fonctions continues de tore. *Journal de théorie des nombres de Bordeaux*, 8(1):205–214, 1996.

[5] François Blanchard and Alejandro Maass. Dynamical properties of expansive one-sided cellular automata. *Israel Journal of Mathematics*, 99(1):149–174, 1997.

[6] Michael D. Boshernitzan. Elementary proof of Furstenberg's diophantine result. *Proceedings of the American Mathematical Society*, 122(1):67–70, 1994.

[7] Tim Boykett and Christopher Moore. Commuting cellular automata. *Complex Systems*, 11(1):55–64, 1997.

[8] Mike Boyle. Open problems in symbolic dynamics. *Contemporary mathematics*, 469:69–118, 2008.

[9] Mike Boyle and Bruce Kitchens. Periodic points for onto cellular automata. *Indagationes Mathematicae*, 10(4):483–493, 1999.

[10] Mike Boyle, Douglas Lind, and Daniel Rudolph. The automorphism group of a shift of finite type. *Transactions of the American Mathematical Society*, 306(1):71–114, 1988.

[11] Yann Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193. Cambridge University Press, 2012.

[12] Van Cyr, John Franks, and Bryna Kra. The spacetime of a shift endomorphism. *Transactions of the American Mathematical Society*, 371(1):461–488, 2019.

[13] Michele D'amico, Giovanni Manzini, and Luciano Margara. On computing the entropy of cellular automata. *Theoretical Computer Science*, 290(3):1629–1646, 2003.

[14] Robert Devaney. *An introduction to chaotic dynamical systems*. CRC Press, 2018.

[15] Sebastián Donoso, Fabien Durand, Alejandro Maass, and Samuel Petite. On automorphism groups of low complexity subshifts. *Ergodic Theory and Dynamical Systems*, 36(1):64–95, 2016.

[16] Artūras Dubickas and Aivaras Novikas. Integer parts of powers of rational numbers. *Mathematische Zeitschrift*, 251(3):635–648, 2005.

[17] Doris Fiebig and Ulf-Rainer Fiebig. The automorphism group of a coded system. *Transactions of the American Mathematical Society*, 348(8):3173–3191, 1996.

[18] Leopold Flatto, Jeffrey C. Lagarias, and Andrew D. Pollington. On the range of fractional parts $\{\xi(p/q)^n\}$. *Acta Arithmetica*, 70(2):125–147, 1995.

[19] W. Forman and H. N. Shapiro. An arithmetic property of certain rational powers. *Communications on Pure and Applied Mathematics*, 20(3):561–573, 1967.

[20] Harry Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation. *Theory of Computing Systems*, 1(1):1–49, 1967.

[21] Pierre Guillon and Ville Salo. Distortion in one-head machines and cellular automata. In *International Workshop on Cellular Automata and Discrete Complex Systems*, pages 120–138. Springer, 2017.

[22] Pierre Guillon and Charalampos Zinoviadis. Densities and entropies in cellular automata. In *Conference on Computability in Europe*, pages 253–263. Springer, 2012.

[23] Yair Hartman. Large semigroups of cellular automata. *Ergodic Theory and Dynamical Systems*, 32(6):1991–2010, 2012.

[24] Gustav A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3(4):320–375, 1969.

[25] Michael Hochman. Non-expansive directions for $\mathbb{Z}^2$ actions. *Ergodic Theory and Dynamical Systems*, 31(1):91–112, 2011.

[26] Lyman P. Hurd, Jarkko Kari, and Karel Culik. The topological entropy of cellular automata is uncomputable. *Ergodic Theory and Dynamical Systems*, 12(2):255–265, 1992.

[27] Joonatan Jalonen and Jarkko Kari. On dynamical complexity of surjective ultimately right-expansive cellular automata. In *International Workshop on Cellular Automata and Discrete Complex Systems*, pages 57–71. Springer, 2018.

[28] Erica Jen. Aperiodicity in one-dimensional cellular automata. *Physica D: Nonlinear Phenomena*, 45(1-3):3–18, 1990.

[29] Uijin Jung. On the existence of open and bi-continuing codes. *Transactions of the American Mathematical Society*, 363(3):1399–1417, 2011.

[30] Jarkko Kari. The nilpotency problem of one-dimensional cellular automata. *SIAM Journal on Computing*, 21(3):571–586, 1992.

[31] Jarkko Kari. Representation of reversible cellular automata with block permutations. *Mathematical Systems Theory*, 29(1):47–61, 1996.

[32] Jarkko Kari. Cellular automata, the Collatz conjecture and powers of 3/2. In *International Conference on Developments in Language Theory*, pages 40–49. Springer, 2012.

[33] Jarkko Kari. Universal pattern generation by cellular automata. *Theoretical Computer Science*, 429:180–184, 2012.

[34] Jarkko Kari. Reversible cellular automata: from fundamental classical results to recent developments. *New Generation Computing*, 36(3):145–172, 2018.

[35] Jarkko Kari and Johan Kopra. Cellular automata and powers of p/q. *RAIRO-Theoretical Informatics and Applications*, 51(4):191–204, 2017.

[36] Bruce P. Kitchens. *Symbolic Dynamics: One-sided, Two-sided and Countable State Markov Shifts*. Springer Science & Business Media, 1997.

[37] Johan Kopra. Glider automorphisms on some shifts of finite type and a finitary Ryan's theorem. In *International Workshop on Cellular Automata and Discrete Complex Systems*, pages 88–99. Springer, 2018.

[38] Johan Kopra. Glider automorphisms and a finitary Ryan's theorem for transitive subshifts of finite type. *Natural Computing*, Sep 2019.

[39] Johan Kopra. The Lyapunov exponents of reversible cellular automata are uncomputable. In *International Conference on Unconventional Computation and Natural Computation*, pages 178–190. Springer, 2019.

[40] Petr Kůrka. Simplicity criteria for dynamical systems. In *Analysis of dynamical and cognitive systems*, pages 189–225. Springer, 1995.

[41] Petr Kůrka. Languages, equicontinuity and attractors in cellular automata. *Ergodic theory and dynamical systems*, 17(2):417–433, 1997.

[42] Petr Kůrka. *Topological and symbolic dynamics*, volume 11. SMF, 2003.

[43] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge university press, 1995.

[44] Ville Lukkarila. *On undecidable dynamical properties of reversible one-dimensional cellular automata*. PhD thesis, University of Turku, 2010.

[45] Kurt Mahler. An unsolved problem on the powers of 3/2. *Journal of the Australian Mathematical Society*, 8(2):313–321, 1968.

[46] Marcus Pivato. Ergodic theory of cellular automata. *Encyclopedia of Complexity and Systems Science*, pages 2980–3015, 2009.

[47] Walter Rudin. *Real and complex analysis*. McGraw-Hill Book Company, New York, 1966.

[48] Daniel J. Rudolph. $\times$ 2 and $\times$ 3 invariant measures and entropy. *Ergodic Theory and Dynamical Systems*, 10(2):395–406, 1990.

[49] J. Patrick Ryan. The shift and commutativity. *Math. Systems Theory*, 6:82–85, 1972.

[50] J. Patrick Ryan. The shift and commutivity. II. *Math. Systems Theory*, 8(3):249–250, 1974/75.

[51] Mathieu Sablik. Directional dynamics for cellular automata: A sensitivity to initial condition approach. *Theoretical Computer Science*, 400(1-3):1–18, 2008.

[52] Ville Salo. *Subshifts with simple cellular automata*. PhD thesis, University of Turku, 2014.

[53] Ville Salo. Transitive action on finite points of a full shift and a finitary Ryan's theorem. *Ergodic Theory Dynam. Systems*, 39(6):1637–1667, 2019.

[54] Ville Salo and Ilkka Törmä. A one-dimensional physically universal cellular automaton. In *Conference on Computability in Europe*, pages 375–386. Springer, 2017.

[55] Mark A. Shereshevsky. Lyapunov exponents for one-dimensional cellular automata. *Journal of Nonlinear Science*, 2(1):1–8, 1992.

[56] M. Shirvani and T.D. Rogers. On ergodic one-dimensional cellular automata. *Communications in mathematical physics*, 136(3):599–605, 1991.

[57] Pierre Tisseur. Cellular automata and Lyapunov exponents. *Nonlinearity*, 13(5):1547, 2000.

[58] Stanislaw M. Ulam. *A collection of mathematical problems*, volume 8. Interscience Publishers, 1960.

[59] Peter Walters. *An introduction to ergodic theory.* Springer-Verlag, New York, 1982.

[60] Hermann Weyl. Über die gleichverteilung von zahlen mod. eins. *Mathematische Annalen*, 77(3):313–352, 1916.

[61] Stephen Wolfram. *A new kind of science*, volume 5. Wolfram media Champaign, IL, 2002.

Turku Centre for Computer Science
TUCS Dissertations

1. **Marjo Lipponen**, On Primitive Solutions of the Post Correspondence Problem
2. **Timo Käkölä**, Dual Information Systems in Hyperknowledge Organizations
3. **Ville Leppänen**, Studies on the Realization of PRAM
4. **Cunsheng Ding**, Cryptographic Counter Generators
5. **Sami Viitanen**, Some New Global Optimization Algorithms
6. **Tapio Salakoski**, Representative Classification of Protein Structures
7. **Thomas Långbacka**, An Interactive Environment Supporting the Development of Formally Correct Programs
8. **Thomas Finne**, A Decision Support System for Improving Information Security
9. **Valeria Mihalache**, Cooperation, Communication, Control. Investigations on Grammar Systems.
10. **Marina Waldén**, Formal Reasoning About Distributed Algorithms
11. **Tero Laihonen**, Estimates on the Covering Radius When the Dual Distance is Known
12. **Lucian Ilie**, Decision Problems on Orders of Words
13. **Jukkapekka Hekanaho**, An Evolutionary Approach to Concept Learning
14. **Jouni Järvinen**, Knowledge Representation and Rough Sets
15. **Tomi Pasanen**, In-Place Algorithms for Sorting Problems
16. **Mika Johnsson**, Operational and Tactical Level Optimization in Printed Circuit Board Assembly
17. **Mats Aspnäs**, Multiprocessor Architecture and Programming: The Hathi-2 System
18. **Anna Mikhajlova**, Ensuring Correctness of Object and Component Systems
19. **Vesa Torvinen**, Construction and Evaluation of the Labour Game Method
20. **Jorma Boberg**, Cluster Analysis. A Mathematical Approach with Applications to Protein Structures
21. **Leonid Mikhajlov**, Software Reuse Mechanisms and Techniques: Safety Versus Flexibility
22. **Timo Kaukoranta**, Iterative and Hierarchical Methods for Codebook Generation in Vector Quantization
23. **Gábor Magyar**, On Solution Approaches for Some Industrially Motivated Combinatorial Optimization Problems
24. **Linas Laibinis**, Mechanised Formal Reasoning About Modular Programs
25. **Shuhua Liu**, Improving Executive Support in Strategic Scanning with Software Agent Systems
26. **Jaakko Järvi**, New Techniques in Generic Programming – C++ is more Intentional than Intended
27. **Jan-Christian Lehtinen**, Reproducing Kernel Splines in the Analysis of Medical Data
28. **Martin Büchi**, Safe Language Mechanisms for Modularization and Concurrency
29. **Elena Troubitsyna**, Stepwise Development of Dependable Systems
30. **Janne Näppi**, Computer-Assisted Diagnosis of Breast Calcifications
31. **Jianming Liang**, Dynamic Chest Images Analysis
32. **Tiberiu Seceleanu**, Systematic Design of Synchronous Digital Circuits
33. **Tero Aittokallio**, Characterization and Modelling of the Cardiorespiratory System in Sleep-Disordered Breathing
34. **Ivan Porres**, Modeling and Analyzing Software Behavior in UML
35. **Mauno Rönkkö**, Stepwise Development of Hybrid Systems
36. **Jouni Smed**, Production Planning in Printed Circuit Board Assembly
37. **Vesa Halava**, The Post Correspondence Problem for Market Morphisms
38. **Ion Petre**, Commutation Problems on Sets of Words and Formal Power Series
39. **Vladimir Kvassov**, Information Technology and the Productivity of Managerial Work
40. **Frank Tétard**, Managers, Fragmentation of Working Time, and Information Systems

41. **Jan Manuch**, Defect Theorems and Infinite Words
42. **Kalle Ranto**, Z_4-Goethals Codes, Decoding and Designs
43. **Arto Lepistö**, On Relations Between Local and Global Periodicity
44. **Mika Hirvensalo**, Studies on Boolean Functions Related to Quantum Computing
45. **Pentti Virtanen**, Measuring and Improving Component-Based Software Development
46. **Adekunle Okunoye**, Knowledge Management and Global Diversity – A Framework to Support Organisations in Developing Countries
47. **Antonina Kloptchenko**, Text Mining Based on the Prototype Matching Method
48. **Juha Kivijärvi**, Optimization Methods for Clustering
49. **Rimvydas Rukšėnas**, Formal Development of Concurrent Components
50. **Dirk Nowotka**, Periodicity and Unbordered Factors of Words
51. **Attila Gyenesei**, Discovering Frequent Fuzzy Patterns in Relations of Quantitative Attributes
52. **Petteri Kaitovaara**, Packaging of IT Services – Conceptual and Empirical Studies
53. **Petri Rosendahl**, Niho Type Cross-Correlation Functions and Related Equations
54. **Péter Majlender**, A Normative Approach to Possibility Theory and Soft Decision Support
55. **Seppo Virtanen**, A Framework for Rapid Design and Evaluation of Protocol Processors
56. **Tomas Eklund**, The Self-Organizing Map in Financial Benchmarking
57. **Mikael Collan**, Giga-Investments: Modelling the Valuation of Very Large Industrial Real Investments
58. **Dag Björklund**, A Kernel Language for Unified Code Synthesis
59. **Shengnan Han**, Understanding User Adoption of Mobile Technology: Focusing on Physicians in Finland
60. **Irina Georgescu**, Rational Choice and Revealed Preference: A Fuzzy Approach
61. **Ping Yan**, Limit Cycles for Generalized Liénard-Type and Lotka-Volterra Systems
62. **Joonas Lehtinen**, Coding of Wavelet-Transformed Images
63. **Tommi Meskanen,** On the NTRU Cryptosystem
64. **Saeed Salehi**, Varieties of Tree Languages
65. **Jukka Arvo**, Efficient Algorithms for Hardware-Accelerated Shadow Computation
66. **Mika Hirvikorpi**, On the Tactical Level Production Planning in Flexible Manufacturing Systems
67. **Adrian Costea**, Computational Intelligence Methods for Quantitative Data Mining
68. **Cristina Seceleanu**, A Methodology for Constructing Correct Reactive Systems
69. **Luigia Petre**, Modeling with Action Systems
70. **Lu Yan**, Systematic Design of Ubiquitous Systems
71. **Mehran Gomari**, On the Generalization Ability of Bayesian Neural Networks
72. **Ville Harkke**, Knowledge Freedom for Medical Professionals – An Evaluation Study of a Mobile Information System for Physicians in Finland
73. **Marius Cosmin Codrea**, Pattern Analysis of Chlorophyll Fluorescence Signals
74. **Aiying Rong**, Cogeneration Planning Under the Deregulated Power Market and Emissions Trading Scheme
75. **Chihab BenMoussa**, Supporting the Sales Force through Mobile Information and Communication Technologies: Focusing on the Pharmaceutical Sales Force
76. **Jussi Salmi**, Improving Data Analysis in Proteomics
77. **Orieta Celiku**, Mechanized Reasoning for Dually-Nondeterministic and Probabilistic Programs
78. **Kaj-Mikael Björk**, Supply Chain Efficiency with Some Forest Industry Improvements
79. **Viorel Preoteasa**, Program Variables – The Core of Mechanical Reasoning about Imperative Programs
80. **Jonne Poikonen**, Absolute Value Extraction and Order Statistic Filtering for a Mixed-Mode Array Image Processor
81. **Luka Milovanov**, Agile Software Development in an Academic Environment
82. **Francisco Augusto Alcaraz Garcia**, Real Options, Default Risk and Soft Applications
83. **Kai K. Kimppa**, Problems with the Justification of Intellectual Property Rights in Relation to Software and Other Digitally Distributable Media
84. **Dragoş Truşcan**, Model Driven Development of Programmable Architectures
85. **Eugen Czeizler**, The Inverse Neighborhood Problem and Applications of Welch Sets in Automata Theory

86. **Sanna Ranto**, Identifying and Locating-Dominating Codes in Binary Hamming Spaces
87. **Tuomas Hakkarainen**, On the Computation of the Class Numbers of Real Abelian Fields
88. **Elena Czeizler**, Intricacies of Word Equations
89. **Marcus Alanen**, A Metamodeling Framework for Software Engineering
90. **Filip Ginter**, Towards Information Extraction in the Biomedical Domain: Methods and Resources
91. **Jarkko Paavola**, Signature Ensembles and Receiver Structures for Oversaturated Synchronous DS-CDMA Systems
92. **Arho Virkki**, The Human Respiratory System: Modelling, Analysis and Control
93. **Olli Luoma**, Efficient Methods for Storing and Querying XML Data with Relational Databases
94. **Dubravka Ilić**, Formal Reasoning about Dependability in Model-Driven Development
95. **Kim Solin**, Abstract Algebra of Program Refinement
96. **Tomi Westerlund**, Time Aware Modelling and Analysis of Systems-on-Chip
97. **Kalle Saari**, On the Frequency and Periodicity of Infinite Words
98. **Tomi Kärki**, Similarity Relations on Words: Relational Codes and Periods
99. **Markus M. Mäkelä**, Essays on Software Product Development: A Strategic Management Viewpoint
100. **Roope Vehkalahti**, Class Field Theoretic Methods in the Design of Lattice Signal Constellations
101. **Anne-Maria Ernvall-Hytönen**, On Short Exponential Sums Involving Fourier Coefficients of Holomorphic Cusp Forms
102. **Chang Li**, Parallelism and Complexity in Gene Assembly
103. **Tapio Pahikkala**, New Kernel Functions and Learning Methods for Text and Data Mining
104. **Denis Shestakov**, Search Interfaces on the Web: Querying and Characterizing
105. **Sampo Pyysalo**, A Dependency Parsing Approach to Biomedical Text Mining
106. **Anna Sell**, Mobile Digital Calendars in Knowledge Work
107. **Dorina Marghescu**, Evaluating Multidimensional Visualization Techniques in Data Mining Tasks
108. **Tero Säntti**, A Co-Processor Approach for Efficient Java Execution in Embedded Systems
109. **Kari Salonen**, Setup Optimization in High-Mix Surface Mount PCB Assembly
110. **Pontus Boström**, Formal Design and Verification of Systems Using Domain-Specific Languages
111. **Camilla J. Hollanti**, Order-Theoretic Mehtods for Space-Time Coding: Symmetric and Asymmetric Designs
112. **Heidi Himmanen**, On Transmission System Design for Wireless Broadcasting
113. **Sébastien Lafond**, Simulation of Embedded Systems for Energy Consumption Estimation
114. **Evgeni Tsivtsivadze**, Learning Preferences with Kernel-Based Methods
115. **Petri Salmela**, On Commutation and Conjugacy of Rational Languages and the Fixed Point Method
116. **Siamak Taati**, Conservation Laws in Cellular Automata
117. **Vladimir Rogojin**, Gene Assembly in Stichotrichous Ciliates: Elementary Operations, Parallelism and Computation
118. **Alexey Dudkov**, Chip and Signature Interleaving in DS CDMA Systems
119. **Janne Savela**, Role of Selected Spectral Attributes in the Perception of Synthetic Vowels
120. **Kristian Nybom**, Low-Density Parity-Check Codes for Wireless Datacast Networks
121. **Johanna Tuominen**, Formal Power Analysis of Systems-on-Chip
122. **Teijo Lehtonen**, On Fault Tolerance Methods for Networks-on-Chip
123. **Eeva Suvitie**, On Inner Products Involving Holomorphic Cusp Forms and Maass Forms
124. **Linda Mannila**, Teaching Mathematics and Programming – New Approaches with Empirical Evaluation
125. **Hanna Suominen**, Machine Learning and Clinical Text: Supporting Health Information Flow
126. **Tuomo Saarni**, Segmental Durations of Speech
127. **Johannes Eriksson**, Tool-Supported Invariant-Based Programming

128. **Tero Jokela**, Design and Analysis of Forward Error Control Coding and Signaling for Guaranteeing QoS in Wireless Broadcast Systems
129. **Ville Lukkarila**, On Undecidable Dynamical Properties of Reversible One-Dimensional Cellular Automata
130. **Qaisar Ahmad Malik**, Combining Model-Based Testing and Stepwise Formal Development
131. **Mikko-Jussi Laakso**, Promoting Programming Learning: Engagement, Automatic Assessment with Immediate Feedback in Visualizations
132. **Riikka Vuokko**, A Practice Perspective on Organizational Implementation of Information Technology
133. **Jeanette Heidenberg**, Towards Increased Productivity and Quality in Software Development Using Agile, Lean and Collaborative Approaches
134. **Yong Liu**, Solving the Puzzle of Mobile Learning Adoption
135. **Stina Ojala**, Towards an Integrative Information Society: Studies on Individuality in Speech and Sign
136. **Matteo Brunelli**, Some Advances in Mathematical Models for Preference Relations
137. **Ville Junnila**, On Identifying and Locating-Dominating Codes
138. **Andrzej Mizera**, Methods for Construction and Analysis of Computational Models in Systems Biology. Applications to the Modelling of the Heat Shock Response and the Self-Assembly of Intermediate Filaments.
139. **Csaba Ráduly-Baka**, Algorithmic Solutions for Combinatorial Problems in Resource Management of Manufacturing Environments
140. **Jari Kyngäs**, Solving Challenging Real-World Scheduling Problems
141. **Arho Suominen**, Notes on Emerging Technologies
142. **József Mezei**, A Quantitative View on Fuzzy Numbers
143. **Marta Olszewska**, On the Impact of Rigorous Approaches on the Quality of Development
144. **Antti Airola**, Kernel-Based Ranking: Methods for Learning and Performace Estimation
145. **Aleksi Saarela**, Word Equations and Related Topics: Independence, Decidability and Characterizations
146. **Lasse Bergroth**, Kahden merkkijonon pisimmän yhteisen alijonon ongelma ja sen ratkaiseminen
147. **Thomas Canhao Xu**, Hardware/Software Co-Design for Multicore Architectures
148. **Tuomas Mäkilä**, Software Development Process Modeling – Developers Perspective to Contemporary Modeling Techniques
149. **Shahrokh Nikou**, Opening the Black-Box of IT Artifacts: Looking into Mobile Service Characteristics and Individual Perception
150. **Alessandro Buoni**, Fraud Detection in the Banking Sector: A Multi-Agent Approach
151. **Mats Neovius**, Trustworthy Context Dependency in Ubiquitous Systems
152. **Fredrik Degerlund**, Scheduling of Guarded Command Based Models
153. **Amir-Mohammad Rahmani-Sane**, Exploration and Design of Power-Efficient Networked Many-Core Systems
154. **Ville Rantala**, On Dynamic Monitoring Methods for Networks-on-Chip
155. **Mikko Pelto**, On Identifying and Locating-Dominating Codes in the Infinite King Grid
156. **Anton Tarasyuk**, Formal Development and Quantitative Verification of Dependable Systems
157. **Muhammad Mohsin Saleemi**, Towards Combining Interactive Mobile TV and Smart Spaces: Architectures, Tools and Application Development
158. **Tommi J. M. Lehtinen**, Numbers and Languages
159. **Peter Sarlin**, Mapping Financial Stability
160. **Alexander Wei Yin**, On Energy Efficient Computing Platforms
161. **Mikołaj Olszewski**, Scaling Up Stepwise Feature Introduction to Construction of Large Software Systems
162. **Maryam Kamali**, Reusable Formal Architectures for Networked Systems
163. **Zhiyuan Yao**, Visual Customer Segmentation and Behavior Analysis – A SOM-Based Approach
164. **Timo Jolivet**, Combinatorics of Pisot Substitutions
165. **Rajeev Kumar Kanth**, Analysis and Life Cycle Assessment of Printed Antennas for Sustainable Wireless Systems
166. **Khalid Latif**, Design Space Exploration for MPSoC Architectures

167. **Bo Yang**, Towards Optimal Application Mapping for Energy-Efficient Many-Core Platforms
168. **Ali Hanzala Khan**, Consistency of UML Based Designs Using Ontology Reasoners
169. **Sonja Leskinen**, m-Equine: IS Support for the Horse Industry
170. **Fareed Ahmed Jokhio**, Video Transcoding in a Distributed Cloud Computing Environment
171. **Moazzam Fareed Niazi**, A Model-Based Development and Verification Framework for Distributed System-on-Chip Architecture
172. **Mari Huova**, Combinatorics on Words: New Aspects on Avoidability, Defect Effect, Equations and Palindromes
173. **Ville Timonen**, Scalable Algorithms for Height Field Illumination
174. **Henri Korvela**, Virtual Communities – A Virtual Treasure Trove for End-User Developers
175. **Kameswar Rao Vaddina**, Thermal-Aware Networked Many-Core Systems
176. **Janne Lahtiranta**, New and Emerging Challenges of the ICT-Mediated Health and Well-Being Services
177. **Irum Rauf**, Design and Validation of Stateful Composite RESTful Web Services
178. **Jari Björne**, Biomedical Event Extraction with Machine Learning
179. **Katri Haverinen**, Natural Language Processing Resources for Finnish: Corpus Development in the General and Clinical Domains
180. **Ville Salo**, Subshifts with Simple Cellular Automata
181. **Johan Ersfolk**, Scheduling Dynamic Dataflow Graphs
182. **Hongyan Liu**, On Advancing Business Intelligence in the Electricity Retail Market
183. **Adnan Ashraf**, Cost-Efficient Virtual Machine Management: Provisioning, Admission Control, and Consolidation
184. **Muhammad Nazrul Islam**, Design and Evaluation of Web Interface Signs to Improve Web Usability: A Semiotic Framework
185. **Johannes Tuikkala**, Algorithmic Techniques in Gene Expression Processing: From Imputation to Visualization
186. **Natalia Díaz Rodríguez**, Semantic and Fuzzy Modelling for Human Behaviour Recognition in Smart Spaces. A Case Study on Ambient Assisted Living
187. **Mikko Pänkäälä**, Potential and Challenges of Analog Reconfigurable Computation in Modern and Future CMOS
188. **Sami Hyrynsalmi**, Letters from the War of Ecosystems – An Analysis of Independent Software Vendors in Mobile Application Marketplaces
189. **Seppo Pulkkinen**, Efficient Optimization Algorithms for Nonlinear Data Analysis
190. **Sami Pyöttiälä**, Optimization and Measuring Techniques for Collect-and-Place Machines in Printed Circuit Board Industry
191. **Syed Mohammad Asad Hassan Jafri**, Virtual Runtime Application Partitions for Resource Management in Massively Parallel Architectures
192. **Toni Ernvall**, On Distributed Storage Codes
193. **Yuliya Prokhorova**, Rigorous Development of Safety-Critical Systems
194. **Olli Lahdenoja**, Local Binary Patterns in Focal-Plane Processing – Analysis and Applications
195. **Annika H. Holmbom**, Visual Analytics for Behavioral and Niche Market Segmentation
196. **Sergey Ostroumov**, Agent-Based Management System for Many-Core Platforms: Rigorous Design and Efficient Implementation
197. **Espen Suenson**, How Computer Programmers Work – Understanding Software Development in Practise
198. **Tuomas Poikela**, Readout Architectures for Hybrid Pixel Detector Readout Chips
199. **Bogdan Iancu**, Quantitative Refinement of Reaction-Based Biomodels
200. **Ilkka Törmä**, Structural and Computational Existence Results for Multidimensional Subshifts
201. **Sebastian Okser**, Scalable Feature Selection Applications for Genome-Wide Association Studies of Complex Diseases
202. **Fredrik Abbors**, Model-Based Testing of Software Systems: Functionality and Performance
203. **Inna Pereverzeva**, Formal Development of Resilient Distributed Systems
204. **Mikhail Barash**, Defining Contexts in Context-Free Grammars
205. **Sepinoud Azimi**, Computational Models for and from Biology: Simple Gene Assembly and Reaction Systems
206. **Petter Sandvik**, Formal Modelling for Digital Media Distribution

207. **Jongyun Moon**, Hydrogen Sensor Application of Anodic Titanium Oxide Nanostructures
208. **Simon Holmbacka**, Energy Aware Software for Many-Core Systems
209. **Charalampos Zinoviadis**, Hierarchy and Expansiveness in Two-Dimensional Subshifts of Finite Type
210. **Mika Murtojärvi**, Efficient Algorithms for Coastal Geographic Problems
211. **Sami Mäkelä**, Cohesion Metrics for Improving Software Quality
212. **Eyal Eshet**, Examining Human-Centered Design Practice in the Mobile Apps Era
213. **Jetro Vesti**, Rich Words and Balanced Words
214. **Jarkko Peltomäki**, Privileged Words and Sturmian Words
215. **Fahimeh Farahnakian**, Energy and Performance Management of Virtual Machines: Provisioning, Placement and Consolidation
216. **Diana-Elena Gratie**, Refinement of Biomodels Using Petri Nets
217. **Harri Merisaari**, Algorithmic Analysis Techniques for Molecular Imaging
218. **Stefan Grönroos**, Efficient and Low-Cost Software Defined Radio on Commodity Hardware
219. **Noora Nieminen**, Garbling Schemes and Applications
220. **Ville Taajamaa**, O-CDIO: Engineering Education Framework with Embedded Design Thinking Methods
221. **Johannes Holvitie**, Technical Debt in Software Development – Examining Premises and Overcoming Implementation for Efficient Management
222. **Tewodros Deneke**, Proactive Management of Video Transcoding Services
223. **Kashif Javed**, Model-Driven Development and Verification of Fault Tolerant Systems
224. **Pekka Naula**, Sparse Predictive Modeling – A Cost-Effective Perspective
225. **Antti Hakkala**, On Security and Privacy for Networked Information Society – Observations and Solutions for Security Engineering and Trust Building in Advanced Societal Processes
226. **Anne-Maarit Majanoja**, Selective Outsourcing in Global IT Services – Operational Level Challenges and Opportunities
227. **Samuel Rönnqvist**, Knowledge-Lean Text Mining
228. **Mohammad-Hashem Hahgbayan**, Energy-Efficient and Reliable Computing in Dark Silicon Era
229. **Charmi Panchal**, Qualitative Methods for Modeling Biochemical Systems and Datasets: The Logicome and the Reaction Systems Approaches
230. **Erkki Kaila**, Utilizing Educational Technology in Computer Science and Programming Courses: Theory and Practice
231. **Fredrik Robertsén**, The Lattice Boltzmann Method, a Petaflop and Beyond
232. **Jonne Pohjankukka**, Machine Learning Approaches for Natural Resource Data
233. **Paavo Nevalainen**, Geometric Data Understanding: Deriving Case-Specific Features
234. **Michal Szabados**, An Algebraic Approach to Nivat's Conjecture
235. **Tuan Nguyen Gia**, Design for Energy-Efficient and Reliable Fog-Assisted Healthcare IoT Systems
236. **Anil Kanduri**, Adaptive Knobs for Resource Efficient Computing
237. **Veronika Suni**, Computational Methods and Tools for Protein Phosphorylation Analysis
238. **Behailu Negash**, Interoperating Networked Embedded Systems to Compose the Web of Things
239. **Kalle Rindell**, Development of Secure Software: Rationale, Standards and Practices
240. **Jurka Rahikkala**, On Top Management Support for Software Cost Estimation
241. **Markus A. Whiteland**, On the k-Abelian Equivalence Relation of Finite Words
242. **Mojgan Kamali**, Formal Analysis of Network Routing Protocols
243. **Jesús Carabaño Bravo**, A Compiler Approach to Map Algebra for Raster Spatial Modeling
244. **Amin Majd**, Distributed and Lightweight Meta-heuristic Optimization Method for Complex Problems
245. **Ali Farooq**, In Quest of Information Security in Higher Education Institutions: Security Awareness, Concerns, and Behaviour of Students
246. **Juho Heimonen**, Knowledge Representation and Text Mining in Biomedical, Healthcare, and Political Domains

247. **Sanaz Rahimi Moosavi**, Towards End-to-End Security in Internet of Things based Healthcare

248. **Mingzhe Jiang**, Automatic Pain Assessment by Learning from Multiple Biopotentials

249. **Johan Kopra**, Cellular Automata with Complicated Dynamics

Turku Centre *for* Computer Science

http://www.tucs.fi

tucs@abo.fi

University of Turku
Faculty of Science and Engineering
- Department of Future Technologies
- Department of Mathematics and Statistics

Turku School of Economics
- Institute of Information Systems Science

Åbo Akademi University
Faculty of Science and Engineering
- Computer Engineering
- Computer Science

Faculty of Social Sciences, Business and Economics
- Information Systems

ISBN 978-952-12-3891-8
ISSN 1239-1883

Johan Kopra Cellular Automata with Complicated Dynamics

Johan Kopra Cellular Automata with Complicated Dynamics

Johan Kopra Cellular Automata with Complicated Dynamics